COMUNE DI CASTELLETTO STURA

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

Aggiornato alle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici in vigore dal 01/01/2022

Sommario

1. Principi generali 7
1.1 PREMESSA 7
1.2 AMBITO DI APPLICAZIONE DEL MANUALE 8
1.3 DEFINIZIONI E NORME DI RIFERIMENTO 8
1.4 AREE ORGANIZZATIVE OMOGENEE E MODELLI ORGANIZZATIVI 9
1.5 ACCREDITAMENTO DELL'AMMINISTRAZIONE ALL'IPA 9
1.6 SERVIZIO PER LA TENUTA DEL PROTOCOLLO INFORMATICO, LA GESTIONE DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI 9
1.7 CASELLE DI POSTA ELETTRONICA 9
1.7.1 Caselle di Posta Elettronica Certificata 9
1.7. 2 Caselle di Posta Elettronica convenzionale 9
1.8 FIRMA DIGITALE 9
1.9 SISTEMA DI CLASSIFICAZIONE DEI DOCUMENTI 10
1.10 TUTELA DEI DATI PERSONALI 10
1.11 FORMAZIONE 10
2. Eliminazione dei protocolli diversi dal protocollo informatico 11
3. Piano di sicurezza dei documenti informatici 12
3.1 OBIETTIVI DEL PIANO DI SICUREZZA 12
3.2 GENERALITÀ 12
4. Modalità di utilizzo di strumenti informatici per la formazione e per lo scambio di documenti informatici 13
4.1 DOCUMENTO RICEVUTO 13
4.2 DOCUMENTO INVIATO 13
4.3 DOCUMENTO INTERNO 13
4.3.1 FORMALE 13
4.3.2 INFORMALE 14
4.5 IL DOCUMENTO INFORMATICO 14
4.6 IL DOCUMENTO ANALOGICO - CARTACEO 14
4.7 FORMAZIONE DEI DOCUMENTI – ASPETTI OPERATIVI 14
4.8 SOTTOSCRIZIONE DI DOCUMENTI INFORMATICI 15
4.9 REQUISITI DEGLI STRUMENTI INFORMATICI DI SCAMBIO 15
4.10 FIRMA DIGITALE 15
4.11 VERIFICA DELLE FIRME CON IL PDP 15

4.12 USO DELLA POSTA ELETTRONICA CERTIFICATA 16
4.13 DESCRIZIONE DI EVENTUALI ULTERIORI FORMATI UTILIZZATI PER LA FORMAZIONE DEL DOCUMENTO INFORMATICO 16
4.14 METADATI ASSOCIATI AI DOCUMENTI SOGGETTI A REGISTRAZIONE 16
5. Descrizione del flusso di lavorazione dei documenti 17
5.1 GENERALITÀ 17
5.2 FLUSSO DEI DOCUMENTI RICEVUTI DALLA AOO 17
5.2.1 PROVENIENZA ESTERNA DEI DOCUMENTI 18
5.2.2 RICEZIONE DI DOCUMENTI INFORMATICI SULLA CASELLA DI POSTA ISTITUZIONALE 18
5.2.3 RICEZIONE DI DOCUMENTI INFORMATICI SU UNA CASELLA DI POSTA ELETTRONICA NON ISTITUZIONALE 18
5.2.4 RICEZIONE DI DOCUMENTI INFORMATICI SU SUPPORTI RIMOVIBILI 18
5.2.5 RICEZIONE DI DOCUMENTI CARTACEI A MEZZO POSTA CONVENZIONALE 18
5.2.6 DOCUMENTI CARTACEI RICEVUTI A MEZZO POSTA CONVENZIONALE E TUTELA DEI DATI PERSONALI 18
5.2.7 ERRATA RICEZIONE DI DOCUMENTI DIGITALI 19
5.2.8 ERRATA RICEZIONE DI DOCUMENTI CARTACEI 19
5.2.9 ATTIVITÀ DI PROTOCOLLAZIONE DEI DOCUMENTI 19
5.2.10 RILASCIO DI RICEVUTE ATTESTANTI LA RICEZIONE DI DOCUMENTI CARTACEI 19
5.2.12 CONSERVAZIONE DELLE RAPPRESENTAZIONI DIGITALI DI DOCUMENTI CARTACEI 19
5.2.13 CLASSIFICAZIONE, ASSEGNAZIONE E PRESA IN CARICO DEI DOCUMENTI 20
5.2.14 CONSERVAZIONE DEI DOCUMENTI NELL'ARCHIVIO CORRENTE 20
5.2.15 CONSERVAZIONE DEI DOCUMENTI E DEI FASCICOLI NELLA FASE CORRENTE 20
5.3 FLUSSO DEI DOCUMENTI INVIATI DALLA AOO 21
5.3.1 VERIFICA FORMALE DEI DOCUMENTI 21
5.3.2 REGISTRAZIONE DI PROTOCOLLO E SEGNATURA 21
5.3.3 TRASMISSIONE DI DOCUMENTI INFORMATICI 21
5.3.4 TRASMISSIONE DI DOCUMENTI CARTACEI A MEZZO POSTA 21
5.3.5 CONTEGGI SPEDIZIONE CORRISPONDENZA 22
5.3.6 DOCUMENTI IN PARTENZA PER POSTA CONVENZIONALE CON PIÙ DESTINATARI 22
5.3.7 TRASMISSIONE DI DOCUMENTI CARTACEI A MEZZO TELEFAX .**Errore. Il segnalibro non è definito.**
6. Regole di smistamento ed assegnazione dei documenti ricevuti 23
6.1 REGOLE DISPONIBILI CON IL PDP 23
6.2 CORRISPONDENZA DI PARTICOLARE RILEVANZA 23
6.3 ASSEGNAZIONE DEI DOCUMENTI RICEVUTI IN FORMATO DIGITALE 23

6.4 ASSEGNAZIONE DEI DOCUMENTI RICEVUTI IN FORMATO CARTACEO 24
6.5 MODIFICA DELLE ASSEGNAZIONI 24
7. Modalità di formazione, implementazione e gestione dei fascicoli informatici 25
7.1 FASCICOLI 25
7.1.1 FASCICOLAZIONE DEI DOCUMENTI 25
7.1.2 APERTURA DEL FASCICOLO 25
7.1.3 CHIUSURA DEL FASCICOLO 25
7.1.4 PROCESSO DI ASSEGNAZIONE DEI FASCICOLI 25
7.1.5 MODIFICA DELLE ASSEGNAZIONI DEI FASCICOLI 26
7.1.6 REPERTORIO DEI FASCICOLI 26
7.2 SERIE ARCHIVISTICHE E REPERTORI 26
7.2.1 SERIE ARCHIVISTICHE 26
7.2.2 REPERTORI E SERIE ARCHIVISTICHE 26
7.2.3 VERSAMENTO DEI FASCICOLI NELL'ARCHIVIO DI DEPOSITO 27
7.2.4 VERIFICA DELLA CONSISTENZA DEL MATERIALE RIVERSATO NELL'ARCHIVIO DI DEPOSITO 27
8. UO responsabili delle attività di registrazione di protocollo, di organizzazione e di tenuta dei documenti 28
9. Elenco dei documenti esclusi dalla protocollazione 28
10. Documenti soggetti a registrazione particolare e registri particolari 29
10.1 REGISTRI PARTICOLARI 29
11. Sistema di classificazione e piano di conservazione 30
11.1 PROTEZIONE E CONSERVAZIONE DEGLI ARCHIVI PUBBLICI 30
11.1.1 GENERALITÀ 30
11.1.2 MISURE DI PROTEZIONE E CONSERVAZIONE DEGLI ARCHIVI PUBBLICI 30
11.2 TITOLARIO O PIANO DI CLASSIFICAZIONE 30
11.2.1 TITOLARIO 30
11.2.2 CLASSIFICAZIONE DEI DOCUMENTI 31
11.3 SCARTO, SELEZIONE E RIORDINO DEI DOCUMENTI 31
11.3.1 OPERAZIONE DI SCARTO 31
11.3.2 CONSERVAZIONE DEL MATERIALE PRESSO LA SEZIONE DI DEPOSITO DELL'ARCHIVIO 31
11.3.3 VERSAMENTO DEI DOCUMENTI NELL'ARCHIVIO STORICO 31
11.4 CONSULTAZIONE E MOVIMENTAZIONE DELL'ARCHIVIO CORRENTE, DI DEPOSITO E STORICO 32
11.4.1 PRINCIPI GENERALI 32
11.4.2 CONSULTAZIONE AI FINI GIURIDICO-AMMINISTRATIVI 32
11.4.3 CONSULTAZIONE PER SCOPI STORICI 33

11.4.4 CONSULTAZIONE DA PARTE DI PERSONALE ESTERNO ALL'AMMINISTRAZIONE 33
11.4.5 CONSULTAZIONE DA PARTE DI PERSONALE INTERNO ALL'AMMINISTRAZIONE..... 33
11.4.6 SCHEMATIZZAZIONE DEL FLUSSO DEI DOCUMENTI ALL'INTERNO DEL SISTEMA ARCHIVISTICO. 34
12. Modalità di produzione e di conservazione delle registrazioni di protocollo informatico 35
12.1 UNICITÀ DEL PROTOCOLLO INFORMATICO..... 35
12.2 REGISTRO GIORNALIERO DI PROTOCOLLO..... 35
Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto. 35
12.3 REGISTRAZIONE DI PROTOCOLLO..... 35
12.4 ELEMENTI FACOLTATIVI DELLE REGISTRAZIONI DI PROTOCOLLO..... 36
12.5 SEGNATURA DI PROTOCOLLO DEI DOCUMENTI..... 36
12.5.1 DOCUMENTI INFORMATICI..... 36
12.5.2 DOCUMENTI CARTACEI RICEVUTI..... 37
12.5.2 DOCUMENTI CARTACEI INVIATI..... 38
12.6 ANNULLAMENTO DELLE REGISTRAZIONI DI PROTOCOLLO..... 38
12.7 LIVELLO DI RISERVATEZZA 38
12.8 CASI PARTICOLARI DI REGISTRAZIONI DI PROTOCOLLO..... 38
12.8.1 PROTOCOLLI RISERVATI..... 38
12.8.2 DOCUMENTI CARTACEI IN PARTENZA CON PIÙ DESTINATARI..... 39
12.8.3 DOCUMENTI CARTACEI RICEVUTI A MEZZO TELEFAX 39
12.8.4 PROTOCOLLAZIONE DI UN NUMERO CONSISTENTE DI DOCUMENTI CARTACEI..... 39
12.8.5 DOCUMENTI INERENTI A GARE DI APPALTO CONFEZIONATI SU SUPPORTI CARTACEI 39
12.8.6 LETTERE ANONIME, PRIVE DI FIRMA O CON FIRMA ILLEGGIBILE 40
12.8.7. MESSAGGI DI POSTA ELETTRONICA CONVENZIONALE 40
12.8.9 RICEZIONE DI DOCUMENTI PERVENUTI ERRONEAMENTE 40
12.8.10 COPIE PER CONOSCENZA DI UN DOCUMENTO CARTACEO..... 40
12.8.11 DIFFERIMENTO DELLE REGISTRAZIONI..... 40
12.8.12 CORRISPONDENZA PERSONALE O RISERVATA 40
12.8.13 INTEGRAZIONI DOCUMENTARIE..... 41
12.8.14 FATTURE ELETTRONICHE (FATTUREPA)..... 41
12.8.15 PRATICHE SUE..... 41
12.8.16 PRATICHE SUAP 41
12.8.17 PRATICHE PRESENTATE TELEMATICAMENTE 42
13. Descrizione funzionale ed operativa del sistema di protocollo informatico..... 43
13.1 DESCRIZIONE FUNZIONALE ED OPERATIVA..... 43

14. Rilascio delle abilitazioni di accesso alle informazioni documentali 44
14.1 GENERALITÀ 44
14.1 RIPRISTINO DELLE CREDENZIALI PRIVATE D'ACCESSO 44
15. Modalità di utilizzo del registro di emergenza 45
15.1 IL REGISTRO DI EMERGENZA 45
15.2 MODALITÀ DI APERTURA DEL REGISTRO DI EMERGENZA 45
15.3 MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA 45
15.4 MODALITÀ DI CHIUSURA E RECUPERO DEL REGISTRO DI EMERGENZA 45
16. Approvazione e aggiornamento del Manuale, norme transitorie e finali 46
16.1 MODALITÀ DI APPROVAZIONE E AGGIORNAMENTO DEL MANUALE 46
16.3 PUBBLICITÀ DEL PRESENTE MANUALE 46
16.4 OPERATIVITÀ DEL PRESENTE MANUALE 46
17. Elenco degli allegati 46

1. Principi generali

1.1 PREMESSA

Il decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 concernente le "*Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005*", all'art. 3, comma 1, lettera d), prevede per tutte le amministrazioni di cui all'art. 2, comma 2, del Codice, l'adozione del Manuale di gestione.
Quest'ultimo, disciplinato dal successivo art. 5, comma 1, "descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi".

Le pubbliche amministrazioni di cui all'art. 2, comma 2, del Codice, nell'ambito del proprio ordinamento, provvedono a individuare le aree organizzative omogenee e i relativi uffici di riferimento ai sensi dell'art. 50 del testo unico e a nominare, in ciascuna delle aree organizzative
omogenee individuate ai sensi dell'art. 50 del Testo unico, il responsabile della gestione documentale, e un suo vicario, per casi di vacanza, assenza o impedimento del primo.

E' compito del responsabile della gestione documentale predisporre lo schema del Manuale di gestione.

Il Manuale di gestione descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Esso disciplina:

- la formazione dei documenti informatici, ai sensi dell'art. 40, comma 1, del Codice, e per lo scambio degli stessi all'interno ed all'esterno dell'area organizzativa omogenea, ivi comprese le caselle di posta elettronica, anche certificata, utilizzate;
- il flusso di lavorazione dei documenti ricevuti, spediti o interni;
- la gestione dei fascicoli informatici relativi ai procedimenti;
- il sistema di classificazione con l'indicazione delle modalità di aggiornamento, integrato con le informazioni relative ai tempi, ai criteri e alle regole di selezione e conservazione, con riferimento alle procedure di scarto;
- la produzione e la conservazione delle registrazioni di protocollo informatico;
- le modalità per il rilascio delle abilitazioni di accesso interno ed esterno alle informazioni documentali;
- l' utilizzo del registro di emergenza ai sensi dell'art. 63 del testo unico, inclusa la funzione di recupero dei dati protocollati manualmente.

Il Manuale di gestione è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le istruzioni complete per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti.

Il presente documento pertanto si rivolge non solo agli operatori di protocollo ma, in generale, a tutti i dipendenti e ai soggetti esterni che si relazionano con l'amministrazione.

1.2 AMBITO DI APPLICAZIONE DEL MANUALE

Il presente Manuale di gestione del protocollo, dei documenti e degli archivi è adottato ai sensi dell'art. 3, comma 1 lettera d) del decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 recante le regole tecniche per il protocollo informatico.

Esso descrive le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre che la gestione dei flussi documentali ed archivistici in relazione ai procedimenti amministrativi del Comune di Castelletto Stura.

Attraverso l'integrazione con le procedure di gestione dei procedimenti amministrativi, di accesso agli atti ed alle informazioni e di archiviazione dei documenti, il protocollo informatico realizza le condizioni operative per una più efficiente gestione del flusso informativo e documentale interno dell'amministrazione anche ai fini dello snellimento delle procedure e della trasparenza dell'azione amministrativa.

Il protocollo fa fede, anche con effetto giuridico, dell'effettivo ricevimento e spedizione di un documento.

1.3 DEFINIZIONI E NORME DI RIFERIMENTO

Ai fini del presente Manuale si intende:
• per "**amministrazione**", il Comune di Castelletto Stura;
• per "**Testo Unico**", il decreto del Presidente della Repubblica 20 dicembre 2000 n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
• per "**Codice**", il decreto legislativo 7 marzo 2005 n. 82 – Codice dell'amministrazione digitale.

Si riportano, di seguito, gli acronimi utilizzati più frequentemente:
• **AOO** - Area Organizzativa Omogenea;
• **MdG** - Manuale di Gestione del protocollo informatico, dei flussi documentali e degli archivi;
• **RPA** - Responsabile del Procedimento Amministrativo - il dipendente che ha la responsabilità dell'esecuzione degli adempimenti amministrativi relativi ad un affare;
• **RGD** - Responsabile della Gestione Documentale ;
• **PdP** - Prodotto di Protocollo informatico – l'applicativo sviluppato o acquisito dall'amministrazione per implementare il servizio di protocollo informatico;
• **UOP** - Unità Organizzative di registrazione di Protocollo - rappresentano gli uffici che svolgono attività di registrazione di protocollo;
• **UOR** - Uffici Organizzativi di Riferimento - un insieme di uffici che, per tipologia di mandato istituzionale e di competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato;
• **UU** - Ufficio Utente - un ufficio dell'AOO che utilizza i servizi messi a disposizione dal sistema di protocollo informatico; ovvero il soggetto destinatario del documento, così come risulta dalla segnatura di protocollo nei campi opzionali.

Ulteriori utili definizioni sono riportate nell'allegato 1.

Per le Norme ed i Regolamenti di riferimento vedasi l'elenco riportato nell'allegato 2.

1.4 AREE ORGANIZZATIVE OMOGENEE E MODELLI ORGANIZZATIVI

Per la gestione dei documenti, l'amministrazione individua un'unica Area Organizzativa Omogenea (AOO) denominata "PROTOCOLLO GENERALE" che è composta dall'insieme di tutti gli UOP/UOR/UU articolati come riportato nell'allegato 3.
All'interno della AOO il sistema di protocollazione è unico ed è centralizzato per la corrispondenza in entrata (salvo rare eccezioni riportate nell'allegato 3), mentre è decentralizzato, per la corrispondenza in uscita, attraverso tutte le UOR che svolgono anche i compiti di UOP. Tale "decentramento" da un punto di vista operativo segue le indicazioni stabilite nel presente Manuale e sarà sottoposto al controllo del RGD.
L'allegato 3 è suscettibile di modifica in caso di inserimento di nuove UOP/UOR/UU o di riorganizzazione delle medesime.

1.5 ACCREDITAMENTO DELL'AMMINISTRAZIONE ALL'IPA

L'amministrazione, nell'ambito degli adempimenti previsti, si è accreditata presso l'Indice delle Pubbliche Amministrazioni (IPA) tenuto e reso pubblico dall' Agenzia per l'Italia.
Le informazioni inerenti all'amministrazione sono riportate nell'allegato 3. L'amministrazione comunica tempestivamente all'IPA ogni successiva modifica.
L'Indice delle Pubbliche Amministrazioni (IPA) è accessibile tramite il relativo sito internet da parte di tutti i soggetti pubblici o privati.

1.6 SERVIZIO PER LA TENUTA DEL PROTOCOLLO INFORMATICO, LA GESTIONE DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

Nell'unica AOO precedentemente individuata è istituito un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi, denominato "Gestione Documentale".
Alla guida del suddetto servizio è posto il Responsabile della Gestione Documentale (di seguito RGD).
L'atto che istituisce il servizio e individua il responsabile è riportato nell'allegato 4.
A tale servizio sono ricondotti i compiti di cui all'art. 61 comma 3 del Testo Unico.

1.7 CASELLE DI POSTA ELETTRONICA

L'elenco completo di tutte le mail attive è pubblicato sul sito dell'amministrazione, nella sezione "Amministrazione trasparente".

1.7.1 Caselle di Posta Elettronica Certificata

L'AOO si è dotata di una casella di Posta Elettronica Certificata istituzionale:
info@pec.comune.castellettostura.cn.it per la corrispondenza, sia in ingresso che in uscita, pubblicata sull'Indice delle Pubbliche Amministrazioni (IPA).
Tale casella costituisce l'indirizzo virtuale della AOO e di tutti gli uffici (UOR) che ad essa fanno riferimento.

Le caselle di Posta Elettronica Certificata sono abilitate a ricevere solo da posta certificata.

1.7. 2 Caselle di Posta Elettronica convenzionale

E' stata inoltre attivata la casella di posta elettronica non certificata (convenzionale) info@comune.castellettostura.cn.it riservata all'invio di messaggi da parte di coloro che non posseggono una PEC.
Ogni dipendente dotato di personal computer ha una casella di posta elettronica non certificata per *comunicazioni informali*.

1.8 FIRMA DIGITALE

Per l'espletamento delle attività istituzionali e per quelle connesse all'attuazione delle norme di gestione del protocollo informatico, di gestione documentale e di archivistica, l'amministrazione fornisce la firma digitale o elettronica qualificata ai soggetti da essa delegati a rappresentarla.
Nell'allegato 5 viene riportato l'elenco delle persone titolari di firma digitale.

1.9 SISTEMA DI CLASSIFICAZIONE DEI DOCUMENTI

La classificazione dei documenti è un'attività di organizzazione di tutti i documenti correnti di un soggetto produttore (ricevuti, spediti, interni) cartacei o informatici, protocollati e non, secondo uno schema articolato di voci che identificano funzioni, attività e materie specifiche del soggetto stesso.

Il piano di classificazione, o titolario, consiste, quindi, in uno schema generale di voci logiche, stabilite in modo uniforme, rispondente alle funzioni – e non alla struttura organizzativa in continua trasformazione – del soggetto produttore e articolate in modo gerarchico.

L'uso del titolario di classificazione permette di organizzare in maniera omogenea e coerente i documenti che si riferiscono ai medesimi affari o ai medesimi procedimenti amministrativi.
Il DPR 445/2000, art.64, c. 4, individua nella classificazione il mezzo per consentire la corretta organizzazione dei documenti, presupposto per il corretto svolgimento dell'attività amministrativa e garanzia del diritto d'accesso ai documenti amministrativi riconosciuta dalla legge 241/1990.

L'amministrazione ha adottato un unico titolario di classificazione per l'unica AOO che identifica l'amministrazione stessa.
Il contenuto della classificazione è dettagliatamente illustrato nel successivo capitolo 9.

1.10 TUTELA DEI DATI PERSONALI

L'amministrazione titolare dei dati di protocollo e dei dati personali - comuni, sensibili e/o giudiziari - contenuti nella documentazione amministrativa di propria pertinenza dà attuazione al dettato del decreto legislativo 30 giugno 2003 n. 196 con atti formali aventi rilevanza interna ed esterna.

Relativamente agli adempimenti interni specifici, gli addetti autorizzati ad accedere al sistema di protocollo informatico e a trattare i dati di protocollo veri e propri, sono stati incaricati dal titolare dei dati e, se nominato, dal responsabile.

Relativamente agli adempimenti esterni, l'amministrazione si è organizzata per garantire che i certificati ed i documenti trasmessi ad altre pubbliche amministrazioni riportino le sole informazioni relative a stati, fatti e qualità personali previste da leggi e regolamenti e strettamente necessarie per il perseguimento delle finalità per le quali vengono acquisite; inoltre l'amministrazione certificante, in caso di accesso diretto ai propri archivi, rilascia all'amministrazione procedente apposita autorizzazione in cui vengono indicati i limiti e le condizioni di accesso volti ad assicurare la riservatezza dei dati personali ai sensi della normativa vigente.

Le regole e le modalità operative stabilite dall'amministrazione sono riportate nel piano di sicurezza di cui al successivo capitolo 3.
In relazione alla protezione dei dati personali trattati al proprio interno l'amministrazione dichiara di aver ottemperato a quanto previsto dal decreto legislativo 30 giugno 2003, n. 196, con particolare riferimento:

- al principio di necessità nel trattamento dei dati;
- al diritto di accesso ai dati personali da parte dell'interessato;
- alle modalità del trattamento e ai requisiti dei dati;
- all'informativa fornita agli interessati ed al relativo consenso quando dovuto;
- alla nomina degli incaricati del trattamento, per gruppo o individualmente;
- alle misure minime di sicurezza.

1.11 FORMAZIONE

Considerato che il personale assegnato agli UOP deve conoscere sia l'organizzazione ed i compiti svolti da ciascun UOR/UU all'interno della AOO sia gli strumenti informatici e le norme di base per la tutela dei dati personali, la raccolta, la registrazione e l'archiviazione delle informazioni, sono previsti specifici percorsi formativi volti ad assicurare la formazione e l'aggiornamento professionale con particolare riferimento:

- ai processi di semplificazione ed alle innovazioni procedurali inerenti alla protocollazione e all'archiviazione dei documenti della AOO;
- agli strumenti e alle tecniche per la gestione digitale delle informazioni, con particolare riguardo alle politiche di sicurezza definite dall'Amministrazione;
- alle norme sulla protezione dei dati personali.

Tali iniziative formative, destinate a specialisti, funzionari e dirigenti dovranno essere previste nel piano annuale di formazione di cui al comma 3 dell'art. 39 del Regolamento sull'ordinamento degli uffici e dei servizi.
Tenute presenti le disponibilità di bilancio, in relazione anche al combinato disposto dell'art. 2 del CCNL 31 marzo 1999 e dell'art. 4 del CCNL 1 aprile 1999, nella impossibilità di organizzare autonomi corsi, è favorita l'adesione a corsi di formazione gratuiti.

2. Eliminazione dei protocolli diversi dal protocollo informatico

In coerenza con quanto previsto e disciplinato, tutti i documenti inviati e ricevuti dall'amministrazione sono registrati all'interno del registro di protocollo informatico. Tutti i registri particolari di protocollo sono stati aboliti ed eliminati.

3. Piano di sicurezza dei documenti informatici

Il Piano di sicurezza dei documenti informatici riporta le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, anche in relazione alle norme sulla protezione dei dati personali.

3.1 OBIETTIVI DEL PIANO DI SICUREZZA

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattati dall'amministrazione siano resi disponibili, integri e riservati;
- i dati personali comuni, sensibili e/o giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

3.2 GENERALITÀ

Il RGD ha fatto predisporre sotto la sua guida e responsabilità il piano di sicurezza dei documenti informatici.

Il piano di sicurezza, che si basa sui risultati dell'analisi dei rischi a cui sono esposti i dati (personali e non), e/o i documenti trattati e sulle direttive strategiche stabilite dal vertice dell'amministrazione, definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno della AOO;
- le modalità di accesso al servizio di protocollo, di gestione documentale ed archivistico;
- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico,con particolare riferimento alle misure minime di sicurezza, *di cui al disciplinare tecnico richiamato nell'allegato b) del decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali*, in caso di trattamento di dati personali.

Il piano di sicurezza è riportato nell'allegato 6.
Le politiche di sicurezza stabiliscono sia le misure preventive per la tutela e l'accesso al patrimonio informativo, sia le misure per la gestione degli incidenti informatici.
È compito del RGD, assistito dal responsabile del sistema informatico, procedere al perfezionamento, alla divulgazione e al riesame e alla verifica delle politiche di sicurezza.
Il riesame delle politiche di sicurezza è conseguente al verificarsi di

- incidenti di sicurezza;
- variazioni tecnologiche significative;
- modifiche all'architettura di sicurezza che potrebbero incidere sulla capacità di mantenere gli obiettivi di sicurezza o portare alla modifica del livello di sicurezza complessivo;
- aggiornamenti delle prescrizioni minime richieste dalla legge in materia di protezione dei dati personali ;
- a seguito dei risultati delle attività di *audit*.

In ogni caso, tale attività è svolta almeno con cadenza annuale.

4. Modalità di utilizzo di strumenti informatici per la formazione e per lo scambio di documenti informatici

Il presente capitolo fornisce indicazioni sulle modalità di utilizzo di strumenti informatici per lo scambio di documenti all'interno ed all'esterno dell'AOO.
Prima di entrare nel merito, occorre caratterizzare l'oggetto di scambio: il documento amministrativo.
Nell'ambito del processo di gestione documentale, il documento amministrativo, in termini operativi, è classificabile in:

- ricevuto;
- inviato;
- interno

Il documento amministrativo, in termini tecnologici, è classificabile in:

- informatico;
- analogico.

4.1 DOCUMENTO RICEVUTO

La corrispondenza in ingresso può essere acquisita dalla AOO con diversi mezzi e modalità in base alla tecnologia di trasporto utilizzata dal mittente.
Un documento informatico può essere recapitato:

- a mezzo posta elettronica convenzionale o certificata;
- su supporto rimovibile quale, ad esempio, *CD ROM, DVD, floppy disk, tape, pen drive*, etc, consegnato direttamente alla UOP o inviato per posta convenzionale o corriere.

Un documento analogico può essere recapitato:

- a mezzo posta convenzionale o corriere;
- a mezzo posta raccomandata;
- per telefax o telegramma;
- con consegna diretta da parte dell'interessato o consegnato tramite una persona dallo stesso delegata alle UOP e/o agli UOR aperti al pubblico.

4.2 DOCUMENTO INVIATO

I documenti informatici, compresi di eventuali allegati, anch'essi informatici, sono inviati, di norma, per mezzo della posta elettronica convenzionale o certificata se la dimensione del documento non supera la dimensione massima prevista dal sistema di posta utilizzato dall'AOO.
In caso contrario, il documento informatico viene riversato, su supporto digitale rimovibile non modificabile e trasmesso con altri mezzi di trasposto al destinatario.

4.3 DOCUMENTO INTERNO

I documenti interni sono formati con tecnologie informatiche e possono essere formali o informali.

4.3.1 FORMALE

Lo scambio tra UOR/UU di documenti informatici di rilevanza amministrativa giuridico-probatoria, avviene di norma tramite PdP (in tal caso i documenti scambiati trovano collocazione sulla scrivania digitale dell'utente destinatario) o in alternativa a mezzo della posta elettronica convenzionale.
Il documento informatico scambiato viene prima sottoscritto con firma digitale e poi protocollato. Entrambe le attività sono svolte tramite PdP.
Nella fase transitoria di migrazione verso la completa gestione informatica dei documenti, il documento interno formale può essere di tipo analogico e lo scambio può aver luogo con i mezzi tradizionali all'interno della AOO. In questo caso il documento viene prodotto con strumenti informatici, stampato e sottoscritto in forma autografa sull'originale, protocollato, scansionato e allegato alla registrazione di protocollo.

4.3.2 INFORMALE

Per questa tipologia di corrispondenza vale quanto illustrato nel paragrafo precedente ad eccezione della obbligatorietà dell'operazione di sottoscrizione e di protocollazione.

4.5 IL DOCUMENTO INFORMATICO

Il documento informatico è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. L'art. 20 del decreto legislativo del 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale" disciplina il documento informatico e in particolare prevede che il documento informatico da chiunque formato, la memorizzazione su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'articolo 71 sono validi e rilevanti agli effetti di legge .
L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità', fermo restando quanto disposto dall'articolo 21 del Codice.

4.6 IL DOCUMENTO ANALOGICO - CARTACEO

Per documento analogico si intende un documento amministrativo "*formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (esempio: documenti cartacei), come le immagini su film (esempio: pellicole mediche, microfiches, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video) su supporto non digitale*".
Di seguito faremo riferimento ad un documento amministrativo cartaceo che può essere prodotto sia in maniera tradizionale (come, ad esempio, una lettera scritta a mano o a macchina), sia con strumenti informatici (ad esempio, una lettera prodotta tramite un sistema di videoscrittura o text editor) e poi stampata.
In quest'ultimo caso si definisce "originale" il documento cartaceo, nella sua redazione definitiva, perfetta ed autentica negli elementi sostanziali e formali comprendente tutti gli elementi di garanzia e di informazione del mittente e destinatario, stampato su carta intestata e dotato di firma autografa.
Si ricorda che l'utilizzo del documento analogico e' residuale, e per lo piu' si riferisce a documentazione desueta.

4.7 FORMAZIONE DEI DOCUMENTI – ASPETTI OPERATIVI

Secondo quanto previsto dall'art. 40 del decreto legislativo n. 82/2005, l'amministrazione forma gli originali dei propri documenti con mezzi informatici.

Ogni documento formato per essere inoltrato all'esterno o all'interno in modo formale:

- tratta un unico argomento indicato in maniera sintetica ma esaustiva a cura dell'autore nello spazio riservato all'oggetto;
- è riferito ad un solo protocollo;
- può far riferimento a più fascicoli.

Le firme *(e le sigle se si tratta di documento analogico)* necessarie alla redazione e perfezione giuridica del documento in partenza devono essere apposte prima della sua protocollazione.
Le regole per la determinazione dei contenuti e della struttura dei documenti informatici sono definite dai responsabili dei singoli UOR.

Il documento deve consentire l'identificazione dell'amministrazione mittente attraverso le seguenti informazioni:

- la denominazione e il logo dell'amministrazione;
- l'indicazione completa della AOO e dell'UOR che ha prodotto il documento;
- l'indirizzo completo dell'amministrazione (via, numero, CAP, città, provincia);
- il numero di telefono della UOR;
- il numero di fax della UOR protocollo;

- il codice fiscale dell'amministrazione.

Il documento deve inoltre recare almeno le seguenti informazioni:

- luogo di redazione del documento;
- la data, (giorno, mese, anno);
- il numero di protocollo;
- il numero di repertorio (se disponibile);
- il numero degli allegati, se presenti;
- l'oggetto del documento;
- se trattasi di documento digitale, firma elettronica avanzata o qualificata da parte dell'istruttore del documento e sottoscrizione digitale del RPA e/o del responsabile del provvedimento finale;
- se trattasi di documento cartaceo, sigla autografa dell'istruttore e sottoscrizione autografa del Responsabile del Procedimento Amministrativo (RPA) e/o del responsabile del provvedimento finale.

4.8 SOTTOSCRIZIONE DI DOCUMENTI INFORMATICI

La sottoscrizione dei documenti informatici, quando prescritta, è ottenuta con un processo di firma digitale conforme alle disposizioni dettate dalla normativa vigente.
L'amministrazione si avvale dei servizi di una autorità di certificazione accreditata, iscritta nell'elenco pubblico dei certificatori accreditati tenuto dall'Agenzia per l'Italia Digitale (AgID).
I documenti informatici prodotti dall'amministrazione, indipendentemente dal software utilizzato per la loro redazione, prima della sottoscrizione con firma digitale, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di archiviazione al fine di garantirne l'immodificabilità (vedi art. 3 comma 3 del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004).

4.9 REQUISITI DEGLI STRUMENTI INFORMATICI DI SCAMBIO

Scopo degli strumenti informatici di scambio e degli standard di composizione dei messaggi è garantire sia l'interoperabilità, sia i requisiti minimi di sicurezza di seguito richiamati:

- l'integrità del messaggio;
- la riservatezza del messaggio;
- il non ripudio dei messaggi;
- l'automazione dei processi di protocollazione e smistamento dei messaggi all'interno delle AOO;
- l'interconnessione tra AOO, ovvero l'interconnessione tra le UOP/UOR e UU di una stessa AOO nel caso di documenti interni formali;
- la certificazione dell'avvenuto inoltro e ricezione;
- l'interoperabilità dei sistemi informativi pubblici.

4.10 FIRMA DIGITALE

Lo strumento che soddisfa i primi tre requisiti di cui al precedente paragrafo 4.9 è la firma digitale utilizzata per inviare e ricevere documenti da e per l'AOO e per sottoscrivere documenti, compresa la copia giornaliera del registro di protocollo e di riversamento, o qualsiasi altro "file" digitale con valenza giuridico-probatoria.
I messaggi ricevuti, sottoscritti con firma digitale, sono sottoposti a verifica di validità.
Tale processo si realizza in modo conforme a quanto prescritto dalla normativa vigente.

4.11 VERIFICA DELLE FIRME CON IL PDP

Nel PdP sono previste funzioni di verifica della firma digitale apposta dall'utente sui documenti e sugli eventuali allegati da fascicolare.

4.12 USO DELLA POSTA ELETTRONICA CERTIFICATA

Lo scambio dei documenti soggetti alla registrazione di protocollo è effettuato mediante messaggi, codificati in formato XML, conformi ai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045-2049 e successive modificazioni o integrazioni.
Il rispetto degli standard di protocollazione, di controllo dei medesimi e di scambio dei messaggi garantisce l'interoperabilità dei sistemi di protocollo (cfr. par. 2.5 Trasmissione e interscambio dei documenti informatici).

Allo scopo di effettuare la trasmissione di un documento da una AOO a un'altra utilizzando l'interoperabilità dei sistemi di protocollo, è necessario eseguire le seguenti operazioni:

- redigere il documento con un sistema di videoscrittura;
- inserire i dati del destinatario (almeno denominazione, indirizzo, casella di posta elettronica);
- firmare il documento (e eventualmente associare il riferimento temporale al documento firmato) e inviare il messaggio contenente il documento firmato digitalmente alla casella interna del protocollo;
- assegnare il numero di protocollo in uscita al documento firmato digitalmente;
- inviare il messaggio contenente il documento firmato e protocollato in uscita alla casella di posta istituzionale del destinatario.

L'utilizzo della Posta Elettronica Certificata (PEC) consente di:

- firmare elettronicamente il messaggio;
- conoscere in modo inequivocabile la data e l'ora di trasmissione;
- garantire l'avvenuta consegna all'indirizzo di posta elettronica dichiarato dal destinatario;
- interoperare e cooperare dal punto di vista applicativo con altre AOO appartenenti alla stessa e ad altre amministrazioni.

Il servizio di Posta Elettronica Certificata è strettamente correlato all'Indice della Pubblica Amministrazione, dove sono pubblicati gli indirizzi istituzionali di posta certificata associati alle AOO.
Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato. La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alla normativa vigente e alle relative regole tecniche sono opponibili ai terzi.
La trasmissione del documento informatico per via telematica, con una modalità che assicuri l'avvenuta consegna, equivale alla notificazione per mezzo della posta nei casi consentiti dalla legge.

4.13 DESCRIZIONE DI EVENTUALI ULTERIORI FORMATI UTILIZZATI PER LA FORMAZIONE DEL DOCUMENTO INFORMATICO

L'amministrazione adotta come standard i formati di cui all'allegato 2 delle regole tecniche per il protocollo informatico, in materia di conservazione e in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni, emanate ai sensi degli articoli 40 -bis , 41, 47, 57 -bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.
Al momento non sono previsti ulteriori formati utilizzati per la formazione del documento informatico.

4.14 METADATI ASSOCIATI AI DOCUMENTI SOGGETTI A REGISTRAZIONE

Con circolare n. 60 del 23 gennaio 2013 l'Agenzia per l'Italia sono definiti formato e definizioni dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le pubbliche amministrazioni. L'amministrazione adotta tale standard.

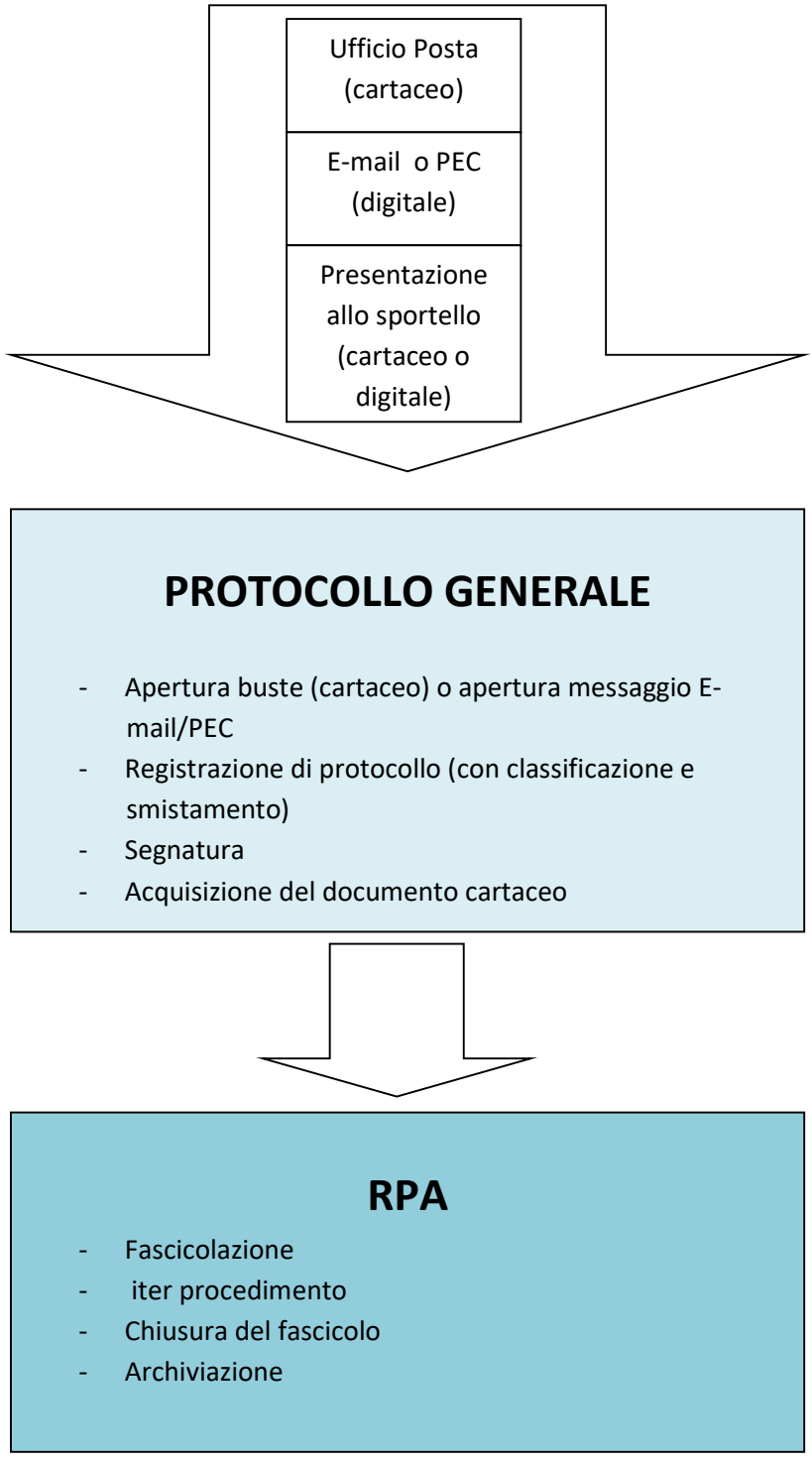
5. Descrizione del flusso di lavorazione dei documenti

Il presente capitolo descrive il flusso di lavorazione dei documenti ricevuti, spediti o interni, incluse le regole di registrazione per i documenti pervenuti secondo particolari modalità di trasmissione.

5.1 GENERALITÀ

Per descrivere i flussi di lavorazione dei documenti all'interno della AOO si fa riferimento ai diagrammi di flussi riportati nelle pagine seguenti.

5.2 FLUSSO DEI DOCUMENTI RICEVUTI DALLA AOO



5.2.1 PROVENIENZA ESTERNA DEI DOCUMENTI

I documenti che transitano attraverso il servizio postale sono consegnati quotidianamente (di norma entro le ore 10) all'UOP da personale delle Poste.

5.2.2 RICEZIONE DI DOCUMENTI INFORMATICI SULLA CASELLA DI POSTA ISTITUZIONALE

La gestione della posta elettronica certificata è integrata nel PdP.
Gli uffici responsabili controllano quotidianamente (possibilmente anche più volte al giorno) i messaggi pervenuti nella casella di posta istituzionale. Ogni messaggio in arrivo è protocollato, archiviato o cestinato.
Nel caso in cui venga recapitato per errore un documento indirizzato ad altro destinatario lo stesso è restituito al mittente con le modalità che saranno successivamente illustrate.

5.2.3 RICEZIONE DI DOCUMENTI INFORMATICI SU UNA CASELLA DI POSTA ELETTRONICA NON ISTITUZIONALE

Nel caso in cui a una casella di posta elettronica *convenzionale diversa da* info@comune.castellettostura.cn.it pervenga un documento da protocollare il messaggio deve essere inoltrato alla casella di posta convenzionale info@comune.castellettostura.cn.it.

5.2.4 RICEZIONE DI DOCUMENTI INFORMATICI SU SUPPORTI RIMOVIBILI

I documenti digitali possono essere recapitati anche per vie diverse dalla posta elettronica.
Considerata l'assenza di standard tecnologici e formali in materia di registrazione di file digitali, la AOO si riserva la facoltà acquisire e trattare tutti i documenti informatici ricevuti su supporto rimovibile che riesce a decodificare e interpretare con le tecnologie a sua disposizione.
Superata questa fase il documento viene inserito nel flusso di lavorazione e sottoposto a tutti i controlli e gli adempimenti del caso.

5.2.5 RICEZIONE DI DOCUMENTI CARTACEI A MEZZO POSTA CONVENZIONALE

I documenti pervenuti a mezzo posta sono consegnati alla UOP.
Le buste o contenitori sono inizialmente esaminati per una preliminare verifica dell'indirizzo e del destinatario sugli stessi apposti.
La corrispondenza relativa a bandi di gara è registrata e successivamente consegnata chiusa all'ufficio responsabile della gara.
La corrispondenza personale non deve essere aperta, né protocollata ma deve essere consegnata al destinatario che ne valuterà il contenuto ed eventualmente, nel caso dovesse riguardare l'istituzione, provvederà a inoltrarla all'ufficio protocollo per la registrazione.
La corrispondenza ricevuta via telegramma o via telefax o le ricevute di ritorno della posta raccomandata, per ciò che concerne la registrazione di protocollo, sono trattate come un documento cartaceo con le modalità descritte nel successivo capitolo 9.
Quando la corrispondenza non rientra nelle categorie da ultimo indicate, si procede all'apertura delle buste e si eseguono gli ulteriori controlli preliminari alla registrazione.
La corrispondenza in arrivo è aperta il giorno lavorativo in cui è pervenuta e contestualmente protocollata. La busta si allega al documento per la parte relativa ai timbri postali.

5.2.6 DOCUMENTI CARTACEI RICEVUTI A MEZZO POSTA CONVENZIONALE E TUTELA DEI DATI PERSONALI

Qualora una AOO sia organizzata per ricevere documenti su carta attraverso qualsiasi UOR aperta al pubblico, oltre, ovviamente alle UOP istituzionali, ovvero se per errore la corrispondenza viene recapitata ad un UOR quest'ultimo, a tutela dei dati personali eventualmente contenuti nella missiva, non apre le buste o i contenitori ricevuti e invia, nella stessa giornata, prima della chiusura del protocollo, la posta a una delle UOP abilitate e "incaricate" dell'apertura della corrispondenza e della protocollazione.
Il personale preposto alla apertura della corrispondenza è stato regolarmente autorizzato al trattamento dei dati personali.

5.2.7 ERRATA RICEZIONE DI DOCUMENTI DIGITALI

Nel caso in cui pervengano sulla casella di posta istituzionale dell'AOO (certificata o meno) o in una casella non istituzionale messaggi dal cui contenuto si rileva che sono stati erroneamente ricevuti, l'operatore di protocollo rispedisce il messaggio al mittente con la dicitura "Messaggio pervenuto per errore - non di competenza di questa AOO".

5.2.8 ERRATA RICEZIONE DI DOCUMENTI CARTACEI

Nel caso in cui pervengano erroneamente alla UOP dell'amministrazione documenti indirizzati ad altri soggetti si restituisce la busta alla posta.
Se la busta viene aperta per errore, il documento è protocollato in entrata e in uscita inserendo nel campo oggetto una nota del tipo "documento pervenuto per errore" e si invia al mittente apponendo sulla busta la dicitura "Pervenuta ed aperta per errore".

5.2.9 ATTIVITÀ DI PROTOCOLLAZIONE DEI DOCUMENTI

Superati tutti i controlli precedenti, i documenti, digitali o analogici, sono protocollati e "segnati" nel protocollo generale secondo gli standard e le modalità dettagliate nel capitolo 9.

5.2.10 RILASCIO DI RICEVUTE ATTESTANTI LA RICEZIONE DI DOCUMENTI CARTACEI

Gli addetti alle UOP non possono rilasciare ricevute per i documenti che non sono soggetti a regolare protocollazione.
La semplice apposizione del timbro datario dell'UOP per la tenuta del protocollo sulla copia, non ha alcun valore giuridico e non comporta alcuna responsabilità del personale dell'UOP in merito alla ricezione ed all'assegnazione del documento.
Quando il documento cartaceo è consegnato direttamente dal mittente o da altra persona incaricata ad una UOP di protocollo ed è richiesto il rilascio di una ricevuta attestante l'avvenuta consegna, la UOP che lo riceve è autorizzata a fotocopiare gratuitamente la prima pagina del documento che su cui è stata posta la segnatura.

5.2.12 CONSERVAZIONE DELLE RAPPRESENTAZIONI DIGITALI DI DOCUMENTI CARTACEI

I documenti ricevuti su supporto cartaceo, dopo le operazioni di registrazione e segnatura, sono acquisiti in formato immagine attraverso un processo di scansione e acquisizione massiva a cura dell'UOP.
Il processo di scansione avviene in diverse fasi:

- acquisizione delle immagini in formato TIFF;
- collegamento alle rispettive registrazioni di protocollo delle immagini in modo tale che ad ogni documento, anche se composto da più pagine, corrisponda un unico file PDF;
- verifica della corretta esecuzione della procedura di archiviazione massiva.

I documenti cartacei, dopo l'operazione di riproduzione in formato PDF, sono inviati agli UOR/UU/RPA destinatari per le operazioni di fascicolazione e conservazione.

I documenti con più destinatari, sono riprodotti in formato immagine ed inviati

- *per competenza* ad un solo ufficio, al quale sarà trasmesso l'originale cartaceo;
- *per conoscenza* ad altri uffici; ai quali sarà trasmesso solo in formato elettronico.

E' consentito far pervenire fotocopia del documento cartaceo originale solo ad assessori o consiglieri comunali che non abbiano fatto richiesta di accesso al PdP.
La riproduzione dei documenti cartacei in formato immagine viene eseguita se il formato del documento ricevuto non supera l'A3.
In ogni caso non vengono riprodotti in formato immagine i seguenti documenti:

- le notifiche del messo e di polizia giudiziaria
- la posta riservata
- il deposito atti.

5.2.13 CLASSIFICAZIONE, ASSEGNAZIONE E PRESA IN CARICO DEI DOCUMENTI

Gli addetti alla UOP eseguono una prima classificazione del documento sulla base del titolario di classificazione adottato presso l'AOO e provvedono ad inviarlo all'UOR di destinazione che:

- esegue una verifica di congruità in base alle proprie competenze;
- in caso di errore, il documento è ritrasmesso alla UOP di origine;
- in caso di verifica positiva, esegue l'operazione di presa in carico smistandola al proprio interno ad UU o direttamente al RPA.

I documenti ricevuti per via telematica sono resi disponibili agli UU, attraverso il PdP, subito dopo l'operazione di smistamento e di assegnazione.
I documenti ricevuti in formato cartaceo di norma sono resi disponibili agli UU in formato digitale, attraverso il PdP, il giorno successivo alla protocollazione.

5.2.14 CONSERVAZIONE DEI DOCUMENTI NELL'ARCHIVIO CORRENTE

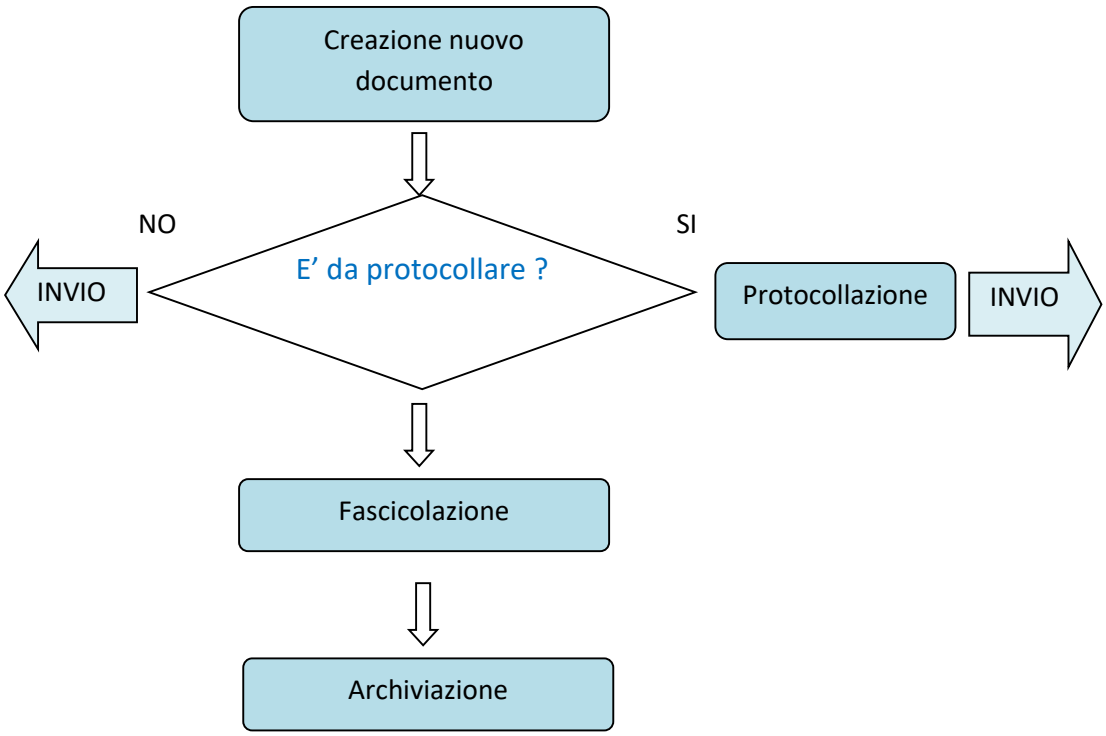
Durante l'ultima fase del flusso di lavorazione della corrispondenza in ingresso vengono svolte le seguenti attività:

1. verifica della prima classificazione del documento effettuata dagli addetti alla UOP ed eventuale sua correzione;
2. fascicolazione del documento secondo le procedure previste dall'AOO;
3. inserimento del fascicolo nel repertorio dei fascicoli nel caso di apertura di un nuovo fascicolo.

5.2.15 CONSERVAZIONE DEI DOCUMENTI E DEI FASCICOLI NELLA FASE CORRENTE

All'interno di ciascun ufficio utente di ciascun UOR della AOO sono stati individuati e formalmente incaricati gli addetti alla organizzazione e tenuta dei fascicoli "attivi" (e chiusi in attesa di riversamento nell'archivio di deposito) e alla conservazione dei documenti al loro interno.
Generalmente i responsabili della conservazione dei documenti e dei fascicoli nella fase corrente sono gli stessi RPA.

5.3 FLUSSO DEI DOCUMENTI INVIATI DALLA AOO



5.3.1 VERIFICA FORMALE DEI DOCUMENTI

Ogni UOR è autorizzata dall'AOO per il tramite del RGD, a svolgere attività di registrazione di protocollo e apposizione della segnatura per la corrispondenza in uscita.
Di conseguenza tutti i documenti originali da spedire, siano essi informatici o analogici, sono direttamente protocollati e spediti dagli UOR.
Gli UOR provvedono ad eseguire al loro interno le verifiche di conformità della documentazione predisposta per essere trasmessa con le stesse modalità descritte nel capitolo precedente.
Se la verifica da esito positivo, il documento viene registrato nel registro di protocollo;

5.3.2 REGISTRAZIONE DI PROTOCOLLO E SEGNATURA

La protocollazione e la segnatura della corrispondenza in partenza, sia essa in formato digitale che in formato analogico, è effettuata direttamente dai singoli RPA/UU/UOR abilitati in quanto collegati al sistema di protocollo informatico della AOO a cui appartengono.
Le attività di registrazione degli elementi obbligatori e degli elementi accessori del protocollo e la relativa segnatura della missiva da inviare sono effettuate dal RPA.

5.3.3 TRASMISSIONE DI DOCUMENTI INFORMATICI

Per la spedizione dei documenti informatici, l'AOO si avvale di un servizio di "Posta Elettronica Certificata", conforme al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.
La trasmissione di un documento informatico, tramite PEC istituzionale, è a cura di chi protocolla, che è tenuto anche a verificarne il corretto invio.

5.3.4 TRASMISSIONE DI DOCUMENTI CARTACEI A MEZZO POSTA

L'UOP generale provvede alle operazioni necessarie per l'invio della corrispondenza in partenza (ad es.: pesatura e affrancatura delle lettere ordinarie, affrancatura delle lettere fuori formato, pesatura, timbratura ed affrancatura posta prioritaria, ricezione e verifica delle distinte di raccomandate compilate ed etichettate dagli uffici, pesatura, affrancatura e registrazioni delle raccomandate estere ecc.).

La corrispondenza da inviare, lettere ordinarie e raccomandate o assicurate, viene consegnata in busta chiusa al servizio postale pubblico di norma alle ore 11,00 di ogni giorno lavorativo (sabato escluso).
Al fine di consentire il regolare svolgimento di tali operazioni, la corrispondenza in partenza deve essere consegnata all'UOP entro e non oltre le ore 10,00 di ogni giorno lavorativo (sabato escluso).
Eventuali situazioni di urgenza saranno valutate dal RGD che potrà autorizzare, in via eccezionale, procedure diverse da quella standard descritta.

5.3.5 CONTEGGI SPEDIZIONE CORRISPONDENZA

L'UOP effettua i conteggi relativi alle spese giornaliere e mensili sostenute per le operazioni di invio della corrispondenza.

5.3.6 DOCUMENTI IN PARTENZA PER POSTA CONVENZIONALE CON PIÙ DESTINATARI

Qualora i destinatari siano più di uno, e comunque in numero maggiore di tre, può essere autorizzata la spedizione di copie dell'originale. L'elenco dei destinatari, in formato cartaceo, è allegato alla minuta.

6. Regole di smistamento ed assegnazione dei documenti ricevuti

Il presente capitolo riporta le regole di smistamento ed assegnazione dei documenti ricevuti.

6.1 REGOLE DISPONIBILI CON IL PDP

L'attività di smistamento consiste nell'operazione di inviare un documento protocollato e segnato all'UOR competente.
Con l'assegnazione si provvede al conferimento della responsabilità del procedimento amministrativo ad un soggetto fisico e alla trasmissione del materiale documentario oggetto di lavorazione.
Effettuato lo smistamento e l'assegnazione, il RPA/UOR competente provvede alla presa in carico del documento allo stesso assegnato.
L'assegnazione può essere effettuata per conoscenza o per competenza.
L'UOR competente è incaricato della gestione del procedimento a cui il documento si riferisce e prende in carico il documento.
I documenti che sono immediatamente riconducibili ad una specifica UOR e/o materia, vengono inoltrati direttamente dalla UOP.
I termini per la definizione del procedimento amministrativo che prende avvio dal documento, decorrono comunque dalla data di protocollazione.
Il sistema di gestione informatica dei documenti memorizza tutti i passaggi, conservando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione.
La traccia risultante definisce, ai fini normativi e regolamentari, i tempi del procedimento amministrativo ed i conseguenti riflessi sotto il profilo della responsabilità.
Nell'allegato 3 sono riportati gli UOR destinatari dello smistamento dei documenti ricevuti dall'AOO e protocollati dall'ufficio Protocollo generale.
Nello stesso allegato, per ciascuna delle strutture in elenco, sono indicati:

- l'indirizzo elettronico;
- le principali tipologie di documenti trattati che determinano i criteri di assegnazione della corrispondenza.

Lo smistamento iniziale eseguito dalla UOP recapita ai dirigenti di ciascuna UOR, attraverso funzioni specifiche del sistema di protocollo informatico, i documenti indirizzati all'UOR medesimo.
Quest'ultimi, dopo averne preso visione, provvedono ad accettarli e ad assegnarli ai propri UU/RPA, oppure, in caso di errore, a rifiutarli (motivando il rifiuto) tramite funzione specifica del PdP o a smistarli direttamente ad altro UOR.

6.2 CORRISPONDENZA DI PARTICOLARE RILEVANZA

Quando un documento pervenuto appare di particolare rilevanza nell'arco della giornata viene inviato in visione al segretario generale affinché possa valutarlo e controllare le assegnazioni suggerite, apportando eventuali modifiche o correzioni.
La corrispondenza ritorna alla UOP per le eventuali correzioni e/o integrazioni.

6.3 ASSEGNAZIONE DEI DOCUMENTI RICEVUTI IN FORMATO DIGITALE

I documenti ricevuti dall'amministrazione in formato digitale, concluse le operazioni di registrazione, di segnatura e di assegnazione, sono resi immediatamente disponibili al RPA/UOR di competenza per via informatica tramite lo strumento "Flussi documentali - scrivania digitale" fornito dallo stesso PdP.
A livello di PdP le attività che possono essere eseguite sul documento sono:

- rifiuto
- presa in carico
- conclusione
- inoltro
- assegnazione.

I destinatari del documento per "competenza" lo ricevono esclusivamente in formato digitale.

6.4 ASSEGNAZIONE DEI DOCUMENTI RICEVUTI IN FORMATO CARTACEO

I documenti ricevuti dall'amministrazione in formato cartaceo, concluse le operazioni di registrazione, di segnatura e di assegnazione e una volta acquisiti in formato immagine con l'ausilio di scanner, sono resi disponibili al RPA/UOR di competenza per via informatica tramite lo strumento "Flussi documentali - scrivania digitale" fornito dallo stesso PdP.
A livello di PdP le attività che possono essere eseguite sul documento sono:

- rifiuto
- presa in carico
- conclusione
- inoltro
- assegnazione.

Di norma la scansione massiva dei documenti e il successivo smistamento dei documenti originali cartacei alle UOR avviene entro la giornata successiva a quella di protocollazione.

6.5 MODIFICA DELLE ASSEGNAZIONI

Nel caso di assegnazione errata, l'UOR/UU che riceve il documento, può provvedere a trasmettere l'atto all'UOR competente oppure può comunicare l'errore (tramite la funzione di rifiuto) alla UOP che ha erroneamente assegnato il documento, che procederà ad una nuova assegnazione.
Il sistema di gestione informatica del protocollo tiene traccia di tutti i passaggi memorizzando l'identificativo dell'utente che effettua l'operazione con la data e l'ora di esecuzione.

7. Modalità di formazione, implementazione e gestione dei fascicoli informatici

7.1 FASCICOLI

7.1.1 FASCICOLAZIONE DEI DOCUMENTI

Tutti i documenti registrati nel sistema informatico e/o classificati, indipendentemente dal supporto sul quale sono formati, sono riuniti in fascicoli.
Ogni documento, dopo la sua classificazione, viene inserito nel fascicolo di riferimento.
I documenti sono archiviati all'interno di ciascun fascicolo o, all'occorrenza, sottofascicolo o inserto, secondo l'ordine cronologico di registrazione.

7.1.2 APERTURA DEL FASCICOLO

Qualora un documento dia luogo all'avvio di un nuovo procedimento amministrativo, si provvede all'apertura di un nuovo fascicolo.
La formazione di un nuovo fascicolo avviene attraverso l'operazione di "apertura" che comprende la registrazione di alcune informazioni essenziali:
• indice di classificazione, (cioè titolo e classe);
• numero del fascicolo;
• oggetto del fascicolo;
• data di apertura del fascicolo;
• UOR;
• collocazione fisica, di eventuali documenti cartacei;
• collocazione logica, dei documenti informatici;
• livello di riservatezza, se diverso da quello standard applicato dal sistema.
Il fascicolo di norma viene aperto all'ultimo livello della struttura gerarchica del titolario.
Le informazioni di cui sopra, compaiono sulla camicia del fascicolo.

7.1.3 CHIUSURA DEL FASCICOLO

Il fascicolo viene chiuso al termine del procedimento amministrativo o all'esaurimento dell'affare.
La data di chiusura si riferisce alla data dell'ultimo documento prodotto.
Esso viene archiviato rispettando l'ordine di classificazione e la data della sua chiusura.

7.1.4 PROCESSO DI ASSEGNAZIONE DEI FASCICOLI

Quando un nuovo documento viene recapitato all'amministrazione, l'UOR abilitato all'operazione di fascicolazione stabilisce, con l'ausilio delle funzioni di ricerca del sistema di protocollo informatizzato, se il documento stesso debba essere ricollegato ad un affare o procedimento in corso, e pertanto debba essere inserito in un fascicolo già esistente, oppure se il documento si riferisce a un nuovo affare o procedimento per cui è necessario aprire un nuovo fascicolo.

A seconda delle ipotesi, si procede come segue:

- Se il documento si ricollega ad un *affare o procedimento in corso*, l'addetto:
  - seleziona il relativo fascicolo;
  - collega la registrazione di protocollo del documento al fascicolo selezionato;
  - invia il documento all'UOR cui è assegnata la pratica. (Se si tratta di un documento su supporto cartaceo, assicura l'inserimento fisico dello stesso nel relativo fascicolo).
- Se il documento dà avvio ad un *nuovo fascicolo*, il soggetto preposto:
  - esegue l'operazione di apertura del fascicolo;
  - collega la registrazione di protocollo del documento al nuovo fascicolo aperto;
  - assegna il documento ad un istruttore su indicazione del responsabile del procedimento;
  - invia il documento con il relativo fascicolo al dipendente che dovrà istruire la pratica per competenza.

7.1.5 MODIFICA DELLE ASSEGNAZIONI DEI FASCICOLI

Quando si verifica un errore nella assegnazione di un fascicolo, l'ufficio abilitato all'operazione di fascicolazione provvede a correggere le informazioni inserite nel sistema informatico e ad inviare il fascicolo all'UOR di competenza.
Il sistema di gestione informatizzata dei documenti tiene traccia di questi passaggi, memorizzando per ciascuno di essi l'identificativo dell'operatore di UU che effettua la modifica con la data e l'ora dell'operazione.

7.1.6 REPERTORIO DEI FASCICOLI

I fascicoli sono annotati nel repertorio dei fascicoli.
Il repertorio dei fascicoli, ripartito per ciascun titolo del titolario, è lo strumento di gestione e di reperimento dei fascicoli.
La struttura del repertorio rispecchia quella del titolario di classificazione e quindi varia in concomitanza con l'aggiornamento di quest'ultimo.
Mentre il titolario rappresenta in astratto le funzioni e le competenze che l'ente può esercitare in base alla propria missione istituzionale, il repertorio dei fascicoli rappresenta in concreto le attività svolte e i documenti prodotti in relazione a queste attività.
Nel repertorio sono indicati:

- la data di apertura;
- l'indice di classificazione completo (titolo, classe, sottoclasse, etc.);
- il numero di fascicolo (ed altre eventuali partizioni in sottofascicoli e inserti);
- la data di chiusura;
- l'oggetto del fascicolo (ed eventualmente l'oggetto dei sottofascicoli e inserti);
- l'annotazione sullo status relativo al fascicolo, se cioè sia ancora una "pratica" corrente, o se abbia esaurito la valenza amministrativa immediata e sia quindi da mandare in deposito, oppure, infine, se sia da scartare o da passare all'archivio storico;
- l'annotazione sullo stato della pratica a cui il fascicolo si riferisce (pratica in corso da inserire nell'archivio corrente, pratica chiusa da inviare all'archivio di deposito, pratica chiusa da inviare all'archivio storico o da scartare).

Il repertorio dei fascicoli è costantemente aggiornato.

7.2 SERIE ARCHIVISTICHE E REPERTORI

7.2.1 SERIE ARCHIVISTICHE

La serie archivistica consiste in un raggruppamento di unità archivistiche (documenti, fascicoli, registri) riunite o per caratteristiche omogenee, quali la natura e la forma dei documenti (es. le determinazioni, i contratti, i registri di protocollo) oppure in base alla materia trattata, all'affare o al procedimento al quale afferiscono (es. i fascicoli personali, le pratiche di finanziamento e in generale le pratiche attivate dall'amministrazione nello svolgimento dell'attività istituzionale).
Le serie documentarie sono formate dai registri e dai relativi fascicoli compresi in un arco d'anni variabile.
I fascicoli subiscono il processo di selezione e scarto dei documenti; le serie così composte, faranno parte, successivamente, della sezione storica dell'archivio.

7.2.2 REPERTORI E SERIE ARCHIVISTICHE

I documenti soggetti a registrazione particolare, come i verbali, le delibere degli organi di governo dell'amministrazione, o i contratti, costituiscono una serie archivistica. Tali documenti sono organizzati nel registro di repertorio.
Con riguardo alla gestione dei documenti cartacei, è previsto che per ogni verbale, delibera, determinazione, decreto, ordinanza e contratto siano, di norma, prodotti almeno due originali, di cui:

- uno viene inserito nel registro di repertorio con il numero progressivo di repertorio;
- l'altro, viene conservato nel relativo fascicolo, insieme ai documenti che afferiscono al medesimo affare o procedimento amministrativo.

Per quanto concerne la gestione dei documenti informatici, ogni verbale, delibera, determinazione, decreto, ordinanza e contratto è, di norma, associato:

- al registro di repertorio con il numero progressivo di repertorio;
- al fascicolo, insieme ai documenti che afferiscono al medesimo affare o procedimento amministrativo.

Nel repertorio generale sono riportati gli elementi obbligatori del documento (data, classifica e numero di repertorio) che identificano il documento all'interno del repertorio stesso.
Il repertorio è costantemente aggiornato.
All'interno dell'amministrazione sono istituiti i repertori generali indicati nell'allegato 10.

7.2.3 VERSAMENTO DEI FASCICOLI NELL'ARCHIVIO DI DEPOSITO

La formazione dei fascicoli (virtuali o tradizionali), delle serie e dei repertori è una funzione fondamentale della gestione archivistica.
Periodicamente, e comunque almeno una volta all'anno, il RGD provvede a trasferire i fascicoli e le serie documentarie relativi ai procedimenti conclusi in un apposita sezione di deposito dell'archivio generale costituito presso l'amministrazione.
Per una regolare e costante "alimentazione" dell'archivio di deposito il RGD stabilisce tempi e modi di versamento dei documenti, organizzati in fascicoli, serie e repertori, dagli archivi correnti dei diversi UOR/UU dell'amministrazione all'archivio di deposito.
Con la stessa metodologia vengono riversati nell'archivio di deposito anche gli altri repertori generali.
La regolare periodicità dell'operazione è fondamentale per garantire l'ordinato sviluppo (o il regolare accrescimento) dell'archivio di deposito.
Il trasferimento deve essere attuato rispettando l'organizzazione che i fascicoli e le serie avevano nell'archivio corrente.
Prima di effettuare il conferimento di cui sopra, il RPA/UU procede alla verifica:

- dell'effettiva conclusione ordinaria della pratica;
- dell'avvenuta annotazione dell'esaurimento della pratica nel registro di repertorio dei fascicoli;
- della corretta indicazione della data di chiusura sulla camicia del fascicolo;

Il RPA/UU provvede inoltre:

- allo scarto di eventuali copie e fotocopie di documentazione di cui è possibile l'eliminazione al fine di garantire la presenza di tutti e soli i documenti relativi alla pratica trattata senza inutili duplicazioni;
- a verificare che il materiale da riversare sia correttamente organizzato e corredato da strumenti che ne garantiscano l'accesso organico.

Ricevuti i fascicoli e controllato l'aggiornamento del relativo repertorio, il RGD predispone un elenco di "versamento" da inviare al servizio archivistico.
Copia di detto elenco viene conservata dal responsabile che ha versato la documentazione.
I fascicoli che riguardano il personale devono essere trasferiti dall'archivio corrente all'archivio di deposito l'anno successivo a quello di cessazione dal servizio.

7.2.4 VERIFICA DELLA CONSISTENZA DEL MATERIALE RIVERSATO NELL'ARCHIVIO DI DEPOSITO

L'ufficio ricevente esegue il controllo del materiale riversato e accetta soltanto i fascicoli con materiale ordinato e completo.
Il fascicolo che in sede di controllo risulta mancante di uno o più documenti ovvero presenti delle incongruenze deve essere restituito agli UOR/UU tenutari dell'archivio corrente, affinché provvedano alla integrazione e/o correzioni necessarie.
Nell'eventualità che non sia stato possibile recuperare uno o più documenti mancanti, il responsabile degli UOR deposita il fascicolo dichiarando ufficialmente che è incompleto e si assume la responsabilità della trasmissione agli atti.
Ricevuti i fascicoli e controllato il relativo elenco, il RGD firma per ricevuta l'elenco di consistenza.

8. UO responsabili delle attività di registrazione di protocollo, di organizzazione e di tenuta dei documenti

Il presente capitolo individua le unità organizzative responsabili delle attività di registrazione di protocollo, di organizzazione e di tenuta dei documenti all'interno della AOO.

In base al modello organizzativo adottato dall'Amministrazione (si veda il par. 1.4 del presente MdG), nell'allegato 3 è riportato l'elenco delle unità organizzative responsabili delle attività di registrazione del protocollo (UOP).

Relativamente alla organizzazione e alla tenuta dei documenti dell'amministrazione all'interno della AOO, è istituito un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi (si veda il par. 1.3 del presente MdG).

9. Elenco dei documenti esclusi dalla protocollazione

Sono esclusi dalla registrazione di protocollo tutti i documenti di cui all'art. 53 comma 5 del decreto del Presidente della Repubblica 20 dicembre 2000, n. 445:

- Gazzette ufficiali
- Bollettini ufficiali e notiziari della pubblica amministrazione
- Note di ricezione delle circolari e altre disposizioni
- Materiali statistici
- Atti preparatori interni
- Giornali e riviste
- Libri
- Materiali pubblicitari
- Inviti a manifestazioni
- Tutti i documenti già soggetti a registrazione particolare dell'amministrazione

Le tipologie di documenti esclusi dalla registrazione di protocollo sono riportati nell'allegato 7.

10. Documenti soggetti a registrazione particolare e registri particolari

10.1 REGISTRI PARTICOLARI

In ambito comunale non sono previsti registri particolari definiti per il trattamento di registrazioni informatiche, albi, elenchi o ogni raccolta di dati concernente stati, qualità personali e fatti, su supporto informatico, in luogo dei registri cartacei.

11. Sistema di classificazione e piano di conservazione

11.1 PROTEZIONE E CONSERVAZIONE DEGLI ARCHIVI PUBBLICI

11.1.1 GENERALITÀ

Il presente capitolo riporta il sistema di classificazione dei documenti, di formazione del fascicolo e di conservazione dell'archivio, con l'indicazione dei tempi e delle modalità di aggiornamento, dei criteri e delle regole di selezione e scarto della documentazione, anche con riferimento all'uso di supporti sostitutivi e di consultazione e movimentazione dei fascicoli.
La classificazione dei documenti, destinata a realizzare una corretta organizzazione dei documenti nell'archivio, è obbligatoria per legge e si avvale del piano di classificazione (titolario), cioè di quello che si suole definire "sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle funzioni dell'ente, al quale viene ricondotta la molteplicità dei documenti prodotti".
Il piano di conservazione, collegato con il titolario ed elaborato tenendo conto dei flussi documentali dipendenti dai procedimenti e dalle prassi seguiti dall'AOO nell'espletamento delle funzioni istituzionali, definisce i tempi di conservazione dei documenti e dei fascicoli nella sezione di deposito dell'archivio.
Il piano di conservazione è riportato nell'allegato 8.

11.1.2 MISURE DI PROTEZIONE E CONSERVAZIONE DEGLI ARCHIVI PUBBLICI

Gli archivi e i singoli documenti degli enti pubblici sono beni culturali inalienabili.
I singoli documenti sopra richiamati (analogici ed informatici, ricevuti, spediti e interni formali) sono quindi inalienabili, sin dal momento dell'inserimento di ciascun documento nell'archivio dell'AOO, di norma mediante l'attribuzione di un numero di protocollo e di un codice di classificazione.
L'archivio non può essere smembrato, a qualsiasi titolo, e deve essere conservato nella sua organicità.
L'archivio di deposito e l'archivio storico non possono essere rimossi dal luogo di conservazione senza l'autorizzazione della soprintendenza archivistica competente per territorio.
Per l'archiviazione e la custodia nella sezione di deposito o storica dei documenti contenenti dati personali, si applicano in ogni caso le disposizioni di legge sulla tutela della riservatezza dei dati personali, sia che si tratti di supporti informatici che convenzionali.

11.2 TITOLARIO O PIANO DI CLASSIFICAZIONE

11.2.1 TITOLARIO

L'amministrazione ha scelto di adottare il titolario proposto dal Gruppo di Lavoro per la formulazione di proposte e modelli per la riorganizzazione dell'archivio dei Comuni (costituito il 18 luglio 2002 con decreto del Direttore Generale per gli archivi) il quale si basa solo su due livelli: i titoli e le classi.
Il piano di classificazione è lo schema logico utilizzato per organizzare i documenti d'archivio in base alle funzioni e alle materie di competenza dell'ente.
Il titolo individua per lo più funzioni primarie e di organizzazione dell'ente (macrofunzioni); le successive classi corrispondono a specifiche competenze che rientrano concettualmente nella macrofunzione descritta dal titolo, articolandosi gerarchicamente tra loro in una struttura ad albero rovesciato, secondo lo schema riportato nell'allegato 9.
Il titolario è uno strumento suscettibile di aggiornamento: esso deve infatti descrivere le funzioni e le competenze dell'ente, soggette a modifiche in forza delle leggi e dei regolamenti statali e/o regionali.
L'aggiornamento del titolario compete esclusivamente al vertice dell'amministrazione, su proposta del RGD.
La revisione anche parziale del titolario viene proposta dal RGD quando è necessario ed opportuno.
Dopo ogni modifica del titolario, il RGD provvede ad informare tutti i soggetti abilitati all'operazione di classificazione dei documenti e a dare loro le istruzioni per il corretto utilizzo delle nuove classifiche.

Il titolario non è retroattivo: non si applica, cioè, ai documenti protocollati prima della sua introduzione.
Viene garantita la storicizzazione delle variazioni di titolario e la possibilità di ricostruire le diverse voci nel tempo mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del titolario vigente al momento della produzione degli stessi.
Per ogni modifica di una voce viene riportata la data di introduzione e la data di variazione.
Di norma le variazioni vengono introdotte a partire dal 1° gennaio dell'anno successivo a quello di approvazione del nuovo titolario e valgono almeno per l'intero anno.
Rimane possibile, se il sistema lo consente, registrare documenti in fascicoli già aperti fino alla conclusione e chiusura degli stessi.

11.2.2 CLASSIFICAZIONE DEI DOCUMENTI

La classificazione è l'operazione finalizzata alla organizzazione dei documenti, secondo un ordinamento logico, in relazione alle funzioni e alle competenze della AOO.
Essa è eseguita a partire dal titolario di classificazione facente parte del piano di conservazione dell'archivio.
Tutti i documenti ricevuti e prodotti dagli UOR dell'AOO, indipendentemente dal supporto sul quale vengono formati, sono classificati in base al sopra citato titolario.
Mediante la classificazione si assegna al documento, oltre al codice completo dell'indice di classificazione (titolo e classe) il numero del fascicolo ed eventualmente del sottofascicolo.

11.3 SCARTO, SELEZIONE E RIORDINO DEI DOCUMENTI

11.3.1 OPERAZIONE DI SCARTO

Nell'ambito della sezione di deposito dell'archivio viene effettuata la selezione della documentazione da conservare perennemente e lo scarto degli atti che l'amministrazione non ritiene più opportuno conservare ulteriormente, allo scopo di conservare e garantire il corretto mantenimento e la funzionalità dell'archivio, nell'impossibilità pratica di conservare indiscriminatamente ogni documento.
Un documento si definisce scartabile quando ha perso totalmente la sua rilevanza amministrativa e non ha assunto alcuna rilevanza storica.
La legge impone all'amministrazione l'uso, *se già esiste*, o la predisposizione di un massimario di selezione e scarto e un piano di conservazione di atti dell'archivio.

11.3.2 CONSERVAZIONE DEL MATERIALE PRESSO LA SEZIONE DI DEPOSITO DELL'ARCHIVIO

L'operazione di riordino della sezione di deposito dell'archivio viene effettuata con la periodicità stabilita dall'amministrazione e consiste nella schedatura dei materiali e nell'organizzazione delle schede.
L'operazione si conclude con la sistemazione fisica del materiale, mediante l'inserimento in unità di condizionamento (es. scatole) che riportano all'esterno l'indicazione del contenuto, la classificazione e i tempi di conservazione dei documenti.

11.3.3 VERSAMENTO DEI DOCUMENTI NELL'ARCHIVIO STORICO

Gli enti pubblici, territoriali e non, trasferiscono al proprio archivio storico i documenti relativi agli affari esauriti da oltre quarant'anni unitamente agli strumenti che ne garantiscono la consultazione.
I trasferimenti vengono effettuati dopo il completamento delle operazioni di scarto.
Presso l'archivio storico i documenti vengono inventariati al fine della conservazione, consultazione e valorizzazione.

11.4 CONSULTAZIONE E MOVIMENTAZIONE DELL'ARCHIVIO CORRENTE, DI DEPOSITO E STORICO

11.4.1 PRINCIPI GENERALI

La richiesta di consultazione, che può comportare la movimentazione dei fascicoli, può pervenire dall'interno dell'amministrazione oppure da utenti esterni all'amministrazione, per scopi giuridico-amministrativi o per scopi storici.

11.4.2 CONSULTAZIONE AI FINI GIURIDICO-AMMINISTRATIVI

Il diritto di accesso ai documenti è disciplinato dall'art. 24 della legge 7 agosto 1990, n. 241 come sostituito dall'art. 16 della legge 11 febbraio 2005, n.15 che qui di seguito si riporta.
"Esclusione dal diritto di accesso.
1. Il diritto di accesso è escluso:
a) per i documenti coperti da segreto di Stato ai sensi della legge 24 ottobre 1977, n. 801, e successive modificazioni, e nei casi di segreto o di divieto di divulgazione espressamente previsti dalla legge, dal regolamento governativo di cui al comma 6 e dalle pubbliche amministrazioni ai sensi del comma 2 del presente articolo;
b) nei procedimenti tributari, per i quali restano ferme le particolari norme che li regolano;
c) nei confronti dell'attività della pubblica amministrazione diretta all'emanazione di atti normativi, amministrativi generali, di pianificazione e di programmazione, per i quali restano ferme le particolari norme che ne regolano la formazione;
d) nei procedimenti selettivi, nei confronti dei documenti amministrativi contenenti informazioni di carattere psicoattitudinale relativi a terzi.
2. Le singole pubbliche amministrazioni individuano le categorie di documenti da esse formati o comunque rientranti nella loro disponibilità sottratti all'accesso ai sensi del comma 1.
3. Non sono ammissibili istanze di accesso preordinate ad un controllo generalizzato dell'operato delle pubbliche amministrazioni.
4. L'accesso ai documenti amministrativi non può essere negato ove sia sufficiente fare ricorso al potere di differimento.
5. I documenti contenenti informazioni connesse agli interessi di cui al comma 1 sono considerati segreti solo nell'ambito e nei limiti di tale connessione. A tale fine le pubbliche amministrazioni fissano, per ogni categoria di documenti, anche l'eventuale periodo di tempo per il quale essi sono sottratti all'accesso.
6. Con regolamento, adottato ai sensi dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400, il Governo può prevedere casi di sottrazione all'accesso di documenti
amministrativi:
a) quando, al di fuori delle ipotesi disciplinate dall'articolo 11. della legge 24 ottobre 1977, n. 801, dalla loro divulgazione possa derivare una lesione, specifica e individuata, alla sicurezza e alla difesa nazionale, all'esercizio della sovranità nazionale e alla continuità e alla correttezza delle relazioni internazionali, con particolare riferimento alle ipotesi previste dai trattati e dalle relative leggi di attuazione;
b) quando l'accesso possa arrecare pregiudizio ai processi di formazione, di determinazione e di attuazione della politica monetaria e valutaria;
c) quando i documenti riguardino le strutture, i mezzi, le dotazioni, il personale e le azioni strettamente strumentali alla tutela dell'ordine pubblico, alla prevenzione e alla repressione della criminalità con particolare riferimento alle tecniche investigative, alla identità delle fonti di informazione e alla sicurezza dei beni e delle persone coinvolte, all'attività di polizia giudiziaria e di conduzione delle indagini;
d) quando i documenti riguardino la vita privata o la riservatezza di persone fisiche, persone giuridiche, gruppi, imprese e associazioni, con particolare riferimento agli interessi epistolare, sanitario, professionale, finanziario, industriale e commerciale di cui siano in concreto titolari, ancorché i relativi dati siano forniti all'amministrazione dagli stessi soggetti cui si riferiscono;
e) quando i documenti riguardino l'attività in corso di contrattazione collettiva nazionale di lavoro e gli atti interni connessi all'espletamento del relativo mandato.

7. Deve comunque essere garantito ai richiedenti l'accesso ai documenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i propri interessi giuridici.
Nel caso di documenti contenenti dati sensibili e giudiziari, l'accesso è consentito nei limiti in cui sia strettamente indispensabile e nei termini previsti dall'articolo 60 del decreto legislativo 30 giugno 2003, n. 196, in caso di dati idonei a rivelare lo stato di salute e la vita sessuale".

11.4.3 CONSULTAZIONE PER SCOPI STORICI

La ricerca per scopi storici è:

- gratuita;
- libera riguardo ai documenti non riservati per legge, per declaratoria del Ministero dell'interno (a norma dell'art. 11.5 del decreto legislativo 22 gennaio 2004, n. 42) o per regolamento emanato dalla stessa amministrazione. È possibile l'ammissione alla consultazione dei documenti riservati, previa autorizzazione rilasciata dal Ministero dell'interno, su conforme parere dell'autorità archivistica competente (Archivio di Stato o soprintendenza archivistica, a seconda che si tratti di archivi statali o non statali);
- condizionata all'accettazione integrale del "codice di deontologia e di buona condotta per il trattamento di dati personali per scopi storici" da parte del soggetto consultatore.

11.4.4 CONSULTAZIONE DA PARTE DI PERSONALE ESTERNO ALL'AMMINISTRAZIONE

La domanda di accesso ai documenti deve essere indirizzata al RGD tramite apposito modulo.
Le domande vengono evase con la massima tempestività e comunque non oltre 10 giorni dalla presentazione.
Con la medesima procedura viene formulata richiesta di accesso alle informazioni raccolte, elaborate ed archiviate in formato digitale.
In tale caso il RGD provvede a consentire l'accesso conformemente a criteri di salvaguardia dei dati dalla distruzione, dalla perdita accidentale, dall'alterazione o dalla divulgazione non autorizzata.
In caso di richieste di consultazione di materiale cartaceo che comportano l'attivazione di ricerche complesse, il termine di evasione della richiesta, di norma, si raddoppia.
L'ingresso all'archivio di deposito e storico è consentito solo agli addetti del servizio archivistico.
La consultazione dei documenti è possibile esclusivamente in un locale appositamente predisposto (aula di studio o di consultazione) sotto la diretta sorveglianza del personale addetto.
Il rilascio di copie dei documenti dell'archivio avviene previo rimborso delle spese di riproduzione, secondo le procedure e le tariffe stabilite dall'amministrazione.
In caso di pratiche momentaneamente irreperibili, in cattivo stato di conservazione, in restauro o in rilegatura, oppure escluse dal diritto di accesso conformemente alla normativa vigente, il responsabile rilascia apposita dichiarazione entro il termine di 30 giorni.

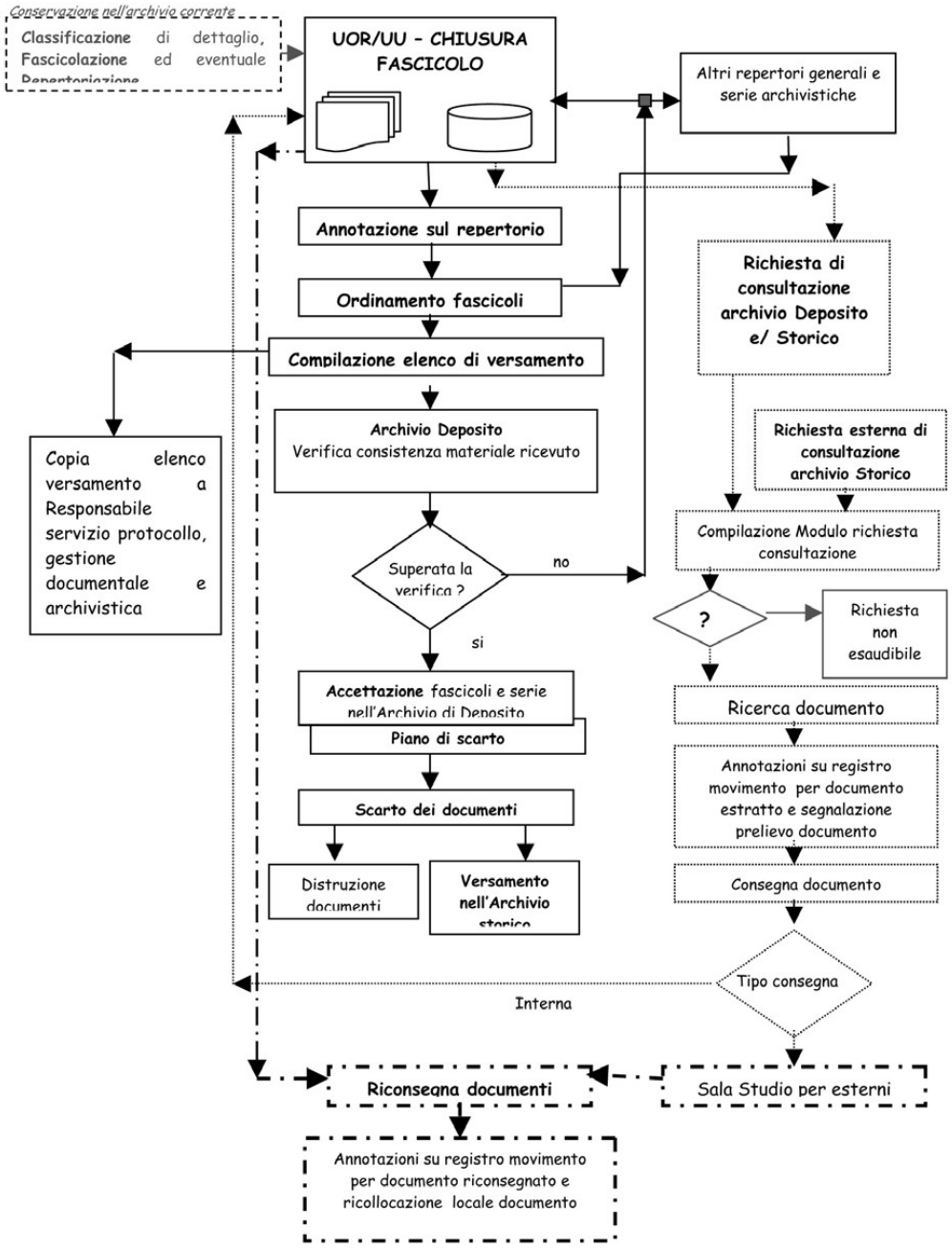
11.4.5 CONSULTAZIONE DA PARTE DI PERSONALE INTERNO ALL'AMMINISTRAZIONE

Gli UOR, per motivi di consultazione, possono richiedere in ogni momento al servizio archivistico i fascicoli conservati nella sezione archivistica di deposito o storica.
L'affidamento temporaneo di un fascicolo già versato all'archivio di deposito o storico ad un ufficio del medesimo UOR/UU od altro UOR/UU avviene solamente per il tempo strettamente necessario all'esaurimento di una procedura o di un procedimento amministrativo.
Nel caso di accesso ad archivi convenzionali cartacei, l'affidamento temporaneo avviene solamente mediante richiesta espressa redatta in duplice copia su un apposito modello, contenente gli estremi identificativi della documentazione richiesta, il nominativo del richiedente, il suo UOR/UU e la sua firma.
Un esemplare della richiesta di consultazione viene conservato all'interno del fascicolo, l'altro nella posizione fisica occupata dal fascicolo in archivio.
Tale movimentazione viene registrata a cura del responsabile del servizio archivistico in un apposito registro di carico e scarico, dove, oltre ai dati contenuti nella richiesta, compaiono la data di consegna/invio e quella di restituzione, nonché eventuali note sullo stato della documentazione in modo da riceverla nello stesso stato in cui è stata consegnata.

Il responsabile del servizio archivistico verifica che la restituzione dei fascicoli affidati temporaneamente avvenga alla scadenza prevista.
L'affidatario dei documenti non estrae i documenti originali dal fascicolo, né altera l'ordine, rispettandone la sedimentazione archivistica e il vincolo.
Nel caso di accesso ad archivi informatici, le formalità da assolvere sono stabilite da adeguate politiche e procedure di accesso alle informazioni stabilite dall'amministrazione.
In ogni caso deve essere garantito l'accesso conformemente a criteri di salvaguardia dei dati dalla distruzione, dalla perdita accidentale, dall'alterazione o dalla divulgazione non autorizzata.

11.4.6 SCHEMATIZZAZIONE DEL FLUSSO DEI DOCUMENTI ALL'INTERNO DEL SISTEMA ARCHIVISTICO

Nella pagina seguente viene riportata una rappresentazione grafica sintetica del complesso delle attività, delle norme e delle responsabilità illustrate nel presente capitolo che, nella loro totalità, costituiscono funzione strategica dell'amministrazione.



12. Modalità di produzione e di conservazione delle registrazioni di protocollo informatico

Il presente capitolo illustra le modalità di produzione e di conservazione delle registrazioni di protocollo informatico, nonché le modalità di registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione.

12.1 UNICITÀ DEL PROTOCOLLO INFORMATICO

Nell'ambito della AOO il registro di protocollo è unico e la numerazione progressiva delle registrazioni di protocollo è unica indipendentemente dal modello organizzativo, centralizzato o distribuito delle UOP, adottato dall'AOO medesima.
La numerazione si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo.
Il numero di protocollo individua un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo.
Il numero di protocollo è costituito da almeno sette cifre numeriche.
Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo che il sistema informatico ha già attribuito ad altri documenti, anche se questi documenti sono strettamente correlati tra loro.
Non è pertanto consentita in nessun caso la cosiddetta registrazione "a fronte", cioè l'utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in partenza.
La documentazione che non è stata registrata presso una UOP viene considerata giuridicamente inesistente presso l'amministrazione.
Non è consentita la protocollazione di un documento già protocollato.
Il registro di protocollo è un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici.
Il registro di protocollo è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.

12.2 REGISTRO GIORNALIERO DI PROTOCOLLO

Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.
A ogni fine giornata il registro giornaliero di protocollo viene automaticamente elaborato nel formato PDF. Se entro la giornata successiva tale file non viene firmato digitalmente dal RGD (o suo delegato) e mandato in conservazione, il sistema procede in automatico a mandarlo in conservazione .

12.3 REGISTRAZIONE DI PROTOCOLLO

Su ogni documento ricevuto o spedito dall'AOO è effettuata una registrazione di protocollo con il sistema di gestione del protocollo informatico, consistente nella memorizzazione dei dati obbligatori.
L'assegnazione delle informazioni nelle operazioni di registrazione di protocollo e' effettuata dal sistema in unica soluzione, con esclusione di interventi intermedi, anche indiretti, da parte dell'operatore, garantendo la completezza dell'intera operazione di modifica o registrazione dei dati.
La registrazione di protocollo per ogni documento ricevuto o spedito dalle pubbliche amministrazioni e' effettuata mediante la memorizzazione delle seguenti informazioni:
a) numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile;
b) data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;
c) mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;
d) oggetto del documento, registrato in forma non modificabile;
e) data e protocollo del documento ricevuto, se disponibili;

f) l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.
La registrazione di protocollo dei documenti informatici ricevuti per posta elettronica è effettuata in modo da far corrispondere ad ogni messaggio una registrazione, la quale si può riferire sia al corpo del messaggio sia ad uno o più file ad esso allegati. Il calcolo dell'impronta previsto nell'operazione di registrazione di protocollo è effettuato per tutti i file allegati al messaggio di posta elettronica ricevuto o inviato.

All'atto della registrazione viene apposto dall'applicativo PdP un riferimento temporale (data e ora).
Il sistema informativo assicura in tal modo la precisione del riferimento temporale con l'acquisizione periodica del tempo ufficiale di rete.

Di seguito vengono illustrate le regole "comuni" di registrazione del protocollo valide per tutti i tipi di documenti trattati dall'AOO (ricevuti, trasmessi ed interni formali, digitali o informatici e analogici).

12.4 ELEMENTI FACOLTATIVI DELLE REGISTRAZIONI DI PROTOCOLLO

Le registrazioni di protocollo, in armonia con la normativa vigente, prevedono elementi accessori, rilevanti sul piano amministrativo, organizzativo e gestionale.
Di seguito vengono riportati gli elementi facoltativi finalizzati alla conservazione e gestione della documentazione:

- data e ora di effettivo ricevimento del documento;
- estremi del documento in ingresso (numero e data);
- data del documento in uscita;
- tipo di posta (consegna a mano, e-mail, e-mail certificata, fax, posta ordinaria, raccomandata, raccomandata A.R., telegramma);
- collegamento a documenti precedenti (originario e padre);
- UOR/UU competente e destinatari delle copie per conoscenza;
- indicazione del livello di sicurezza se diverso da quello standard applicato dal sistema di protocollazione;
- classificazione del documento (titolo, classe e fascicolo);

Il RGD, con proprio provvedimento e al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa, può modificare e integrare gli elementi facoltativi del protocollo.
La registrazione degli elementi facoltativi del protocollo può essere modificata, integrata e cancellata in base alle effettive esigenze delle UOR o degli UOP.
I dati facoltativi sono modificabili senza necessità di annullare la registrazione di protocollo, fermo restando che il sistema informatico di protocollo registra tali modifiche.

12.5 SEGNATURA DI PROTOCOLLO DEI DOCUMENTI

L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione di protocollo.
La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso.
Essa consente di individuare ciascun documento in modo inequivocabile.

12.5.1 DOCUMENTI INFORMATICI

I dati relativi alla segnatura di protocollo di un documento trasmesso da una area organizzativa omogenea sono associati al documento stesso e contenuti, nel messaggio, in un file, conforme alle specifiche dell'Extensible Markup Language (XML), compatibile con un file XML Schema e/o DTD (Document Type Definition), definito e aggiornato periodicamente dall'Agenzia per l'Italia digitale con provvedimento reso disponibile sul proprio sito.

Con tale provvedimento sono altresì definiti e aggiornati periodicamente gli standard, le modalità di trasmissione, il formato e le definizioni dei tipi di informazioni scambiate tra le amministrazioni pubbliche e associate ai documenti protocollati.
La struttura ed i contenuti del file di segnatura di protocollo di un documento informatico sono conformi alle disposizioni tecniche vigenti.
Le informazioni minime incluse nella segnatura sono quelle di seguito elencate:

- codice identificativo dell'amministrazione;
- codice identificativo dell'area organizzativa omogenea;
- codice identificativo del registro;
- data di protocollo;
- progressivo di protocollo secondo il formato specificato all'art. 57 del testo unico;
- oggetto;
- mittente;
- il destinatario o i destinatari.

E' facoltativo riportare anche le seguenti informazioni:

- indicazione della persona o dell'ufficio all'interno della struttura destinataria a cui si presume verrà affidato il trattamento del documento;
- indice di classificazione;
- identificazione degli allegati;
- informazioni sul procedimento a cui si riferisce e sul trattamento da applicare al documento.

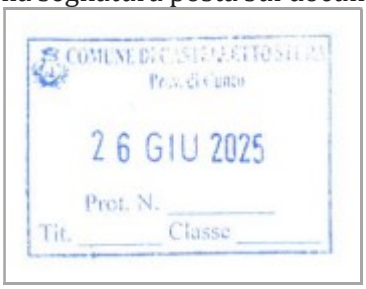
L'AOO che riceve il documento informatico può utilizzare tali informazioni per automatizzare le operazioni di registrazione di protocollo del documento ricevuto.
Qualora l'AOO decida di scambiare con altre AOO informazioni non previste tra quelle definite come facoltative, può estendere il file di cui sopra, includendo le informazioni specifiche stabilite di comune accordo, nel rispetto delle indicazioni tecniche stabilite dall'Agenzia per l'Italia digitale.

12.5.2 DOCUMENTI CARTACEI RICEVUTI

La segnatura di protocollo di un documento cartaceo ricevuto avviene attraverso l'apposizione su di esso di un timbro.
Sul timbro vengono riportate le seguenti informazioni relative alla registrazione di protocollo:

- l'identificazione dell'amministrazione : "COMUNE DI CASTELLETTO STURA";
- la data di protocollo;
- il numero di protocollo (costituito da 7 cifre numeriche);
- l'indice di classificazione (titolo e classe);

L'acquisizione dei documenti può essere eseguita solo dopo l'operazione di segnatura.
Di seguito è riportato un facsimile della segnatura posta sui documenti in arrivo:



Di norma la segnatura di protocollo deve essere apposto sulla prima pagina dell'originale.
Se il documento non presenta spazi sufficienti per l'applicazione del timbro, essa viene apposto sul retro della prima pagina dell'originale

12.5.2 DOCUMENTI CARTACEI INVIATI

La segnatura di protocollo di un documento cartaceo inviato avviene apponendo direttamente sul documento, redatto su carta intestata individuante l'amministrazione comunale, il numero di protocollo.
L'immagine del documento, firmato con firma autografa e protocollato, viene acquisita dopo la segnatura e allegata alla registrazione di protocollo.

12.6 ANNULLAMENTO DELLE REGISTRAZIONI DI PROTOCOLLO

L'annullamento anche di una sola delle informazioni generate o assegnate automaticamente dal sistema e registrate in forma immodificabile determina l'automatico e contestuale annullamento della intera registrazione di protocollo.
L'annullamento anche di un solo campo delle altre informazioni registrate in forma immodificabile, necessario per correggere errori intercorsi in sede di immissione di dati delle altre informazioni, deve comportare la rinnovazione del campo stesso con i dati corretti e la contestuale memorizzazione, in modo permanente, del valore precedentemente attribuito unitamente alla data, l'ora e all'autore della modifica.
Le informazioni relative alla registrazione di protocollo annullata rimangono memorizzate nel registro informatico del protocollo per essere sottoposte alle elaborazioni previste dalla procedura, ivi comprese le visualizzazioni e le stampe, nonché la data, l'ora e l'autore dell'annullamento e gli estremi dell'autorizzazione all'annullamento del protocollo rilasciata dal RGD.
In tale ipotesi la procedura riporta la dicitura "annullato" in posizione visibile e tale, da consentire la lettura di tutte le informazioni originarie. Il sistema registra l'avvenuta rettifica, la data ed il soggetto che è intervenuto.
Solo il RGD è autorizzato ad annullare, ovvero a dare disposizioni di annullamento delle registrazioni di protocollo.
L'annullamento di una registrazione di protocollo generale deve essere richiesto con specifica nota, adeguatamente motivata, indirizzata al RGD.
A tal fine è istituito un registro informatico per le richieste di annullamento delle registrazioni.
Il registro riporta i motivi dell'annullamento e, se il documento è stato protocollato nuovamente, il nuovo numero di protocollo assegnato.

12.7 LIVELLO DI RISERVATEZZA

L'operatore che effettua la registrazione di protocollo di un documento attribuisce allo stesso il livello di riservatezza che ritiene necessario, se diverso da quello standard applicato automaticamente dal sistema.
In modo analogo, il RPA che effettua l'operazione di apertura di un nuovo fascicolo ne fissa anche il livello di riservatezza.
Il livello di riservatezza applicato ad un fascicolo è acquisito automaticamente da tutti i documenti che vi confluiscono, se a questi è stato assegnato un livello di riservatezza minore od uguale. I documenti che invece hanno un livello di riservatezza superiore lo mantengono.

12.8 CASI PARTICOLARI DI REGISTRAZIONI DI PROTOCOLLO

12.8.1 PROTOCOLLI RISERVATI

All'interno dell'AOO è "istituito" il protocollo riservato - sottratto alla consultazione da parte di chi non sia espressamente abilitato - nel quale sono riportati:

- documenti relativi a vicende di persone o a fatti privati o particolari;
- documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obbiettivi prefissati;
- documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa.

I documenti (informatici o cartacei) anonimi, *come tali individuati ai sensi dell'art. 8, comma 4, e 141 del codice di procedura penale*, vengono inviati al RGD che ne effettua una valutazione:

- se ritiene che contengano dati o informazioni di interesse dell'amministrazione, provvede ad inviarli agli uffici competenti per le ulteriori eventuali determinazioni.
  Questi decidono se registrarli, farli registrare nel protocollo generale;
- se ritiene che non contengano dati rilevanti dal punto di vista amministrativo, il documento viene registrato nel protocollo riservato.

Negli archivi cartacei, il protocollo riservato è un piccolo complesso di documenti tenuti sotto chiave, tenuto personalmente dal responsabile a ciò autorizzato.
L'introduzione del protocollo unico informatico, e l'intervento in esso di più persone autorizzate ad operare, è compatibile con rigorose misure di tutela del protocollo riservato.
Quest'ultimo comporta modalità non ordinarie di registrazione per i documenti che oggettivamente richiedono particolari cautele di riservatezza; esso può essere consentito a pochi rappresentanti dell'Ente appositamente autorizzati, e vincolati ovviamente al segreto.
Tale tipo eccezionale di registrazione è da collocarsi all'interno della catena numerica del protocollo informatico generale, ma con modalità tali da rendere uno o più campi non visibili agli impiegati addetti al normale protocollo.

12.8.2 DOCUMENTI CARTACEI IN PARTENZA CON PIÙ DESTINATARI

Qualora i destinatari siano più di uno, è autorizzata la spedizione di copie dell'originale.
Nella registrazione di protocollo come destinatario deve essere indicato la dicitura "Destinatari vari".
Nell'apposita sezione delle note va indicato " Vedi elenco allegato".
I destinatari sono indicati in appositi elenchi da associare alla minuta del documento e alla registrazione di protocollo.

12.8.3 DOCUMENTI CARTACEI RICEVUTI A MEZZO TELEFAX

L'uso del telefax soddisfa il requisito della forma scritta e, quindi, il documento può non essere seguito dalla trasmissione dell'originale.
Nel caso in cui al telefax segua l'originale, poiché ogni documento va identificato da un solo numero di protocollo, è necessario che all'originale sia attribuita la medesima segnatura di protocollo.
Se si accerta che l' originale è stato registrato con un numero diverso, si procede all'annullamento della registrazione dell'originale.
Se tra il telefax e l'originale ricevuto successivamente vi sono differenze, anche minime, essi debbono essere considerati documenti diversi, aventi quindi protocollazione distinta.
Il timbro di protocollo va apposto sul documento e non sulla copertina di trasmissione del telefax.

12.8.4 PROTOCOLLAZIONE DI UN NUMERO CONSISTENTE DI DOCUMENTI CARTACEI

Quando si presenti la necessità di protocollare un numero consistente di documenti, sia in ingresso (es. scadenza gare o concorsi) che in uscita, deve esserne data comunicazione all'ufficio protocollo con almeno due giorni lavorativi di anticipo, onde concordare tempi e modi di protocollazione e di spedizione.

12.8.5 DOCUMENTI INERENTI A GARE DI APPALTO CONFEZIONATI SU SUPPORTI CARTACEI

La corrispondenza che riporta l'indicazione "offerta" - "gara d'appalto" - "preventivo" o simili, o dal cui involucro è possibile evincere che si riferisce alla partecipazione ad una gara, non deve essere aperta, ma protocollata in arrivo con l'apposizione della segnatura, della data e dell'ora e dei minuti di registrazione direttamente sulla busta, plico o simili, e deve essere inviata all'UOR competente.
È compito dello stesso UOR provvedere alla custodia delle buste o dei contenitori protocollati, con mezzi idonei, sino all'espletamento della gara stessa.
Dopo l'apertura delle buste l'UOR che gestisce la gara d'appalto riporta gli estremi di protocollo indicati sulla confezione esterna su tutti i documenti in essa contenuti.
Per motivi organizzativi tutti gli UOR sono tenuti ad informare preventivamente l'UOP generale dell'amministrazione in merito alle scadenze di concorsi, gare, bandi di ogni genere.

12.8.6 LETTERE ANONIME, PRIVE DI FIRMA O CON FIRMA ILLEGGIBILE

Il registro di protocollo è un atto pubblico che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso.
In base a questo principio sono da protocollare le lettere anonime, prive di firma o con firma illeggibile.
È poi compito dell'UOR di competenza e, in particolare, del RPA valutare, se il documento privo di firma debba ritenersi valido e come tale trattato dall'ufficio assegnatario.
Le lettere anonime saranno registrate, ponendo come mittente la dicitura "Mittente sconosciuto o anonimo".

12.8.7. MESSAGGI DI POSTA ELETTRONICA CONVENZIONALE

Considerato che l'attuale sistema di posta elettronica non certificata non consente una sicura individuazione del mittente, questa tipologia di corrispondenza è trattata nei seguenti modi:

- in caso di invio, come allegato, di un documento scansionato e munito di firma autografa, quest'ultimo è trattato come un documento inviato via fax fermo restando che l'RPA deve verificare la provenienza certa dal documento; in caso di mittente non verificabile, l'RPA valuta caso per caso l'opportunità di trattare il documento inviato via e-mail;
- in caso di invio, in allegato, di un documento munito di firma digitale, o di invio di un messaggio firmato con firma digitale, il documento e/o il messaggio sono considerati come un documento elettronico inviato con qualunque mezzo di posta;
- in caso di invio di una e-mail contenente un testo non sottoscritto quest'ultima sarà considerata come missiva anonima.

12.8.9 RICEZIONE DI DOCUMENTI PERVENUTI ERRONEAMENTE

Nel caso in cui sia protocollato un documento erroneamente inviato all'amministrazione, l'addetto al protocollo provvede o ad annullare il protocollo stesso.
Il documento viene restituito al mittente.

12.8.10 COPIE PER CONOSCENZA DI UN DOCUMENTO CARTACEO

Chi effettua la registrazione e lo smistamento dell'originale e delle copie, inserisce nel registro di protocollo i nominativi di coloro ai quali sono state inviate le suddette copie per conoscenza.
Sulla segnatura di protocollo è indicato unicamente il destinatario dell'originale.
I nominativi di coloro ai quali sono state inviate le suddette copie per conoscenza è riportato manualmente sull'originale.

12.8.11 DIFFERIMENTO DELLE REGISTRAZIONI

Le registrazioni di protocollo dei documenti pervenuti presso l'amministrazione destinataria sono effettuate nella giornata di arrivo e comunque non oltre le 48 ore dal ricevimento di detti documenti.
Qualora non possa essere effettuata la registrazione di protocollo nei tempi sopra indicati si provvede a protocollare, in via prioritaria, i documenti che rivestono una particolare importanza.
Il differimento dei termini di registrazione si applica solo ai documenti in arrivo.
Sui documenti viene apposto un timbro attestante la data di effettivo arrivo.

12.8.12 CORRISPONDENZA PERSONALE O RISERVATA

La corrispondenza personale è regolarmente aperta dagli uffici incaricati della registrazione di protocollo dei documenti in arrivo, a meno che sulla busta non sia riportata la dicitura "riservata" o "personale".
In quest'ultimo caso, la corrispondenza con la dicitura "riservata" o "personale" non è aperta ed è consegnata in busta chiusa al destinatario, il quale, dopo averne preso visione, se reputa che i documenti ricevuti devono essere comunque protocollati provvede a trasmetterli all'ufficio abilitato alla registrazione di protocollo dei documenti in arrivo.

12.8.13 INTEGRAZIONI DOCUMENTARIE

L'addetto al protocollo non è tenuto a controllare la completezza formale e sostanziale della documentazione pervenuta.
Tale verifica spetta al Responsabile del Procedimento Amministrativo (RPA) che, qualora reputi necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente indicando con precisione l'indirizzo al quale inviarli e specificando che la mancata integrazione della documentazione pervenuta comporta l'interruzione o la sospensione del procedimento.
I documenti pervenuti ad integrazione di quelli già disponibili sono protocollati dalla UOP sul protocollo generale e, a cura del RPA, sono inseriti nel fascicolo relativo.

12.8.14 FATTURE ELETTRONICHE (FATTUREPA)

Per legge è la sola tipologia di fattura accettata dalle Amministrazioni che, sono tenute ad avvalersi del Sistema di Interscambio.
Ha le seguenti caratteristiche:

- il contenuto è rappresentato, in un file XML (eXtensible Markup Language), secondo il formato della FatturaPA. Questo formato è l' unico accettato dal Sistema di Interscambio (SdI).
- l' autenticità dell' origine e l' integrità del contenuto sono garantite tramite l' apposizione della firma elettronica qualificata di chi emette la fattura,
- la trasmissione è vincolata alla presenza del codice identificativo univoco dell'ufficio destinatario della fattura, riportato nell' Indice delle Pubbliche Amministrazioni.

Tutte le fatture elettroniche pervengono all'indirizzo info@comune.castellettostura.cn.it, vengono protocollate in automatico e smistate direttamente sulle scrivanie digitali delle varie UOR/UU in funzione del codice unico dell'ufficio che ha ordinato la fornitura/prestazione indicato in fattura.
I codici sono elencati nell'allegato 3.
Compete ad ogni UOR effettuare l'accettazione o il rifiuto (motivato) di una fattura elettronica entro i 15 gg dalla ricezione della stessa, tramite lo stesso Pdp.
Una volta accettate le fatture vengono salvate in una cartella appositamente creata e condivisa perché possano essere poi importate dal gestionale in uso agli uffici finanziari.

12.8.15 PRATICHE SUE

E' obbligatoria la presentazione telematica attraverso il portale dello "Sportello unico digitale" delle pratiche di

- Comunicazione di Inizio Lavori (CIL),
- Comunicazione di Inizio Lavori Asseverata (CILA),
- Segnalazione Certificata di Inizio Attività (SCIA),
- Rilascio del certificato di agibilità.

Rimane in vigore la tradizionale presentazione su carta, all'ufficio protocollo generale, delle altre istanze: permesso di costruire, autorizzazione paesaggistica, ecc.,

12.8.16 PRATICHE SUAP

La presentazione deve essere effettuata telematicamente attraverso il portale dello "Sportello unico digitale" per

- Segnalazione Certificata di Inizio Attività (SCIA),
- Denuncia di inizio attività in edilizia (DIA),
- Autorizzazione Unica Ambientale (AUA),
- Comunicazioni, per le quali risultano disponibili le procedure e la modulistica online,
- Pratiche di prevenzione incendi,
- Pratiche relative agli impianti radioelettrici,
- Pratiche relative alle attività economiche afferenti l'esercizio delle stesse (avvio, cessazione, variazione, notifiche sanitarie, ecc.).

La presentazione delle domande di procedimento ordinario per il rilascio di atti autorizzativi complessi può essere effettuata telematicamente, ovvero in forma cartacea per le pratiche più articolate o che presentano criticità; in questi casi è meglio contattare preliminarmente gli uffici.

12.8.17 PRATICHE PRESENTATE TELEMATICAMENTE

Tutte le pratiche presentate telematicamente attraverso il portale dello “Sportello unico digitale” vengono protocollate automaticamente e smistate sulla scrivania dell’UOR.
Le pratiche SUAP e SUE vengono importate dall’UOR nel relativo gestionale.

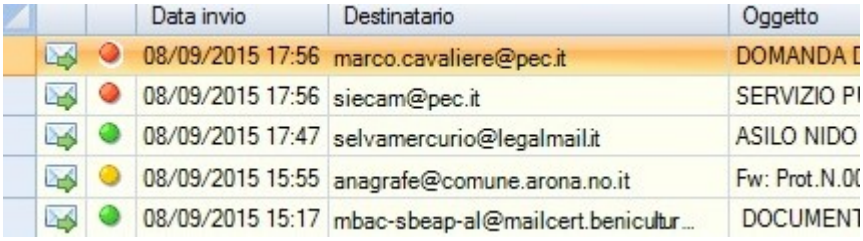
13. Descrizione funzionale ed operativa del sistema di protocollo informatico

Il presente capitolo contiene la descrizione funzionale ed operativa del sistema di protocollo informatico adottato dall'amministrazione con particolare riferimento alle modalità di utilizzo dello stesso.
Il sistema di protocollo informatico in uso è GM Protocollo Informatico di Technical Design di Cuneo.

13.1 DESCRIZIONE FUNZIONALE ED OPERATIVA

Di seguito viene fornita una elencazione sintetica delle principali funzioni del PdP.
Possiamo identificare quattro moduli:

- **Protocollo informatico**
  Raggruppa le funzioni per la gestione e consultazione del protocollo informatico (dalla registrazione alla ricerca) e le funzioni per la gestione della casella mail info@comune.castellettostura.cn.it e della PEC info@pec.comune.castellettostura.cn.it
  Ogni messaggio in arrivo a queste caselle è protocollato, archiviato o cestinato.
  Per ogni PEC inviata è possibile monitorarne lo stato:
  - bollino verde vuol dire che è stata accettata e consegnata;
  - bollino giallo che si ha solo certezza dell'avvenuta partenza (tipicamente invio a una casella e-mail convenzionale);
  - bollino rosso che la mail non è neppure stata accettata.



- **Flussi documentali**
  Tramite lo strumento "scrivania digitale" vengono gestiti i flussi documentali.
  Tutti i documenti in arrivo vengono assegnati agli UOR di competenza, che vedono sulla propria scrivania digitale il documento protocollato sotto forma di "attività assegnata".
  Gli operatori possono rifiutare l'attività (perché non di propria competenza), prenderla in carica (tipicamente il documento richiede una risposta o dà inizio ad un procedimento) o concluderla (il documento richiede solo presa visione o è stata fornita in qualche modo una risposta).
  L'attività può essere altresì inoltrata ad altra UOR o assegnata ad una precisa persona dell'ufficio.
  Il sistema tiene traccia di ogni passaggio.
  Dalla scrivania digitale è anche possibile inserire il documento in un fascicolo ed effettuare accettazione e rifiuto delle fatture elettroniche.
- **Fascicoli documentali**
  Raggruppa le funzioni per la gestione dei fascicoli documentali (dalla creazione alla ricerca)
- **Caselle E-mail/PEC**
  Raggruppa le funzioni per la gestione delle altre caselle e-mail/PEC indicate nell'indice PA:
  - tecnico@comune.castellettostura.cn.it

  A queste caselle dovrebbero pervenire per lo più solo messaggi provenienti da trasmissione telematica e come tali già protocollati, ma poiché potrebbero arrivare anche messaggi da altri canali, si tratta di monitorare la posta in arrivo per inoltrare tali messaggi ad altre caselle o per protocollarli.
  Nell'allegato 11 è riportata, per motivi di opportunità, la descrizione dettagliata di dette funzioni.

14. Rilascio delle abilitazioni di accesso alle informazioni documentali

Il presente capitolo riporta i criteri e le modalità per il rilascio delle abilitazioni di accesso interno ed esterno alle informazioni documentali gestite dal PdP.

14.1 GENERALITÀ

Il controllo degli accessi è il processo che garantisce l'impiego degli oggetti/servizi del sistema informatico di protocollo esclusivamente secondo modalità prestabilite.
Il processo è caratterizzato da utenti che accedono ad oggetti informatici (applicazioni, dati, programmi) mediante operazioni specifiche (lettura, aggiornamento, esecuzione).
Gli utenti del servizio di protocollo, in base agli UU di appartenenza, ovvero in base alle rispettive competenze (UOP, UOR, UU) hanno autorizzazioni di accesso differenziate in base alle tipologie di operazioni stabilite dall'ufficio di appartenenza.
Ad ogni utente è assegnata:

- una credenziale di accesso costituita da una componente:
  – pubblica che permette l'identificazione dell'utente da parte del sistema (*userID*);
  – privata o riservata di autenticazione (*password*);
- una autorizzazione di accesso (profilo) al fine di limitare le operazioni di protocollo e gestione documentale alle sole funzioni necessarie e indispensabili a svolgere le attività di competenza dell'ufficio a cui l'utente appartiene.

I diversi livelli di autorizzazione sono assegnati agli utenti dal RGD tramite l'ufficio Sistemi informatici.
Questi le autorizzazioni previste per tipologia di utente (profili) :

	Visualizzazione	Inserimento	Modifica	Annullamento	Visualizzazione completa registro protocollo
Personale ufficio protocollo generale	X	X	X		X
Personale ufficio Sistemi Informatici (Ruolo di amministratore)	X	X	X	X	X
Operatore protocollo altro ufficio	X	X	X		
Operatore di sola consultazione	X				

14.1 RIPRISTINO DELLE CREDENZIALI PRIVATE D'ACCESSO

Nel caso in cui un operatore di protocollo dimentichi la password di accesso al PdP può richiederne il reset all'ufficio Sistemi Informatici.

15. Modalità di utilizzo del registro di emergenza

Il presente capitolo illustra le modalità di utilizzo del registro di emergenza, inclusa la funzione di recupero dei dati protocollati manualmente, prevista dal PdP.

15.1 IL REGISTRO DI EMERGENZA

Il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi autorizza lo svolgimento anche manuale delle operazioni di registrazione di protocollo su uno o più registri di emergenza, ogni qualvolta per cause tecniche non sia possibile utilizzare la normale procedura informatica.

15.2 MODALITÀ DI APERTURA DEL REGISTRO DI EMERGENZA

Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema.
La protocollazione di emergenza va effettuata esclusivamente presso l'Ufficio Protocollo generale.
Le operazioni di protocollo sono svolte manualmente sul registro di emergenza, sia esso cartaceo o informatico, su postazioni di lavoro operanti fuori linea.
Il formato delle registrazioni di protocollo, ovvero i campi obbligatori delle registrazioni, sono quelli stessi previsti dal protocollo generale.
Qualora l'impossibilita' di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore, per cause di eccezionale gravità, il responsabile per la tenuta del protocollo può autorizzare l'uso del registro di emergenza per periodi successivi di non più di una settimana.

15.3 MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

Per ogni giornata di registrazione di emergenza è riportato sul relativo registro il numero totale di operazioni registrate manualmente.
Durante il periodo di interruzione del servizio di protocollo informatico generale, il responsabile del sistema informatico (o persona da lui delegata) provvede a tener informato il RGD sui tempi di ripristino del servizio.

15.4 MODALITÀ DI CHIUSURA E RECUPERO DEL REGISTRO DI EMERGENZA

È compito del RGD verificare la chiusura del registro di emergenza.
Una volta ripristinata la piena funzionalità del PdP, il RGD provvede alla chiusura del registro di emergenza annotando, sullo stesso il numero delle registrazioni effettuate e la data e ora di chiusura.
Dopo la chiusura del registro di emergenza gli utenti potranno tornare a protocollare regolarmente.
È compito del RGD, o suo delegato, riportare dal registro di emergenza al sistema di protocollo generale (PdP) le protocollazioni relative ai documenti protocollati manualmente, entro cinque giorni dal ripristino delle funzionalità del sistema.
Le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, utilizzando un'apposita funzione di recupero dei dati, senza ritardo al ripristino delle funzionalità del sistema.
Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza.
La sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'area organizzativa omogenea.
Il registro di emergenza si configura come un repertorio del protocollo generale.
Ad ogni registrazione recuperata dal registro di emergenza viene attribuito un nuovo numero di protocollo generale, continuando la numerazione del protocollo generale raggiunta al momento dell'interruzione del servizio.

16. Approvazione e aggiornamento del Manuale, norme transitorie e finali

16.1 MODALITÀ DI APPROVAZIONE E AGGIORNAMENTO DEL MANUALE

L'amministrazione adotta il presente "Manuale di gestione" su proposta del responsabile della gestione documentale (RGD).
Il presente Manuale potrà essere aggiornato a seguito di:

- normativa sopravvenuta;
- introduzione di nuove pratiche tendenti a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza;
- inadeguatezza delle procedure rilevate nello svolgimento delle attività correnti;
- modifiche apportate negli allegati dal RGD.

16.3 PUBBLICITÀ DEL PRESENTE MANUALE

Il presente Manuale, a norma dell'art. 22 della legge 7 agosto 1900, n. 241, è reso disponibile alla consultazione del pubblico che ne può prendere visione in qualsiasi momento.
Inoltre copia del presente Manuale è:

- resa disponibile a tutto il personale dell'AOO mediante la rete intranet;
- pubblicata sul sito internet dell'amministrazione.

16.4 OPERATIVITÀ DEL PRESENTE MANUALE

Il presente regolamento è operativo il primo giorno del mese successivo a quello della sua approvazione.
Con l'entrata in vigore del presente Manuale è annullato il Manuale di gestione e conservazione dei documenti adottato con delibera della Giunta Comunale n. 89 del 10 giugno 2004.

17. Elenco degli allegati

1. DEFINIZIONI
2. NORMATIVA DI RIFERIMENTO
3. AREE ORGANIZZATIVE OMOGENEE E MODELLO ORGANIZZATIVO
4. ATTO DI NOMINA DEL RESPONSABILE DELLA GESTIONE DOCUMENTALE
5. ELENCO DELLE PERSONE TITOLARI DI FIRMA DIGITALE
6. POLITICHE DI SICUREZZA
7. ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO
8. PIANO DI CONSERVAZIONE
9. TITOLARIO DI CLASSIFICAZIONE
10. REPERTORI GENERALI
11. DESCRIZIONE FUNZIONALE ED OPERATIVA DEL PRODOTTO DI PROTOCOLLO (PDP) INFORMATICO IN USO PRESSO L'AREA ORGANIZZATIVA OMOGENEA

Allegato 1

DEFINIZIONI

AMMINISTRAZIONI CERTIFICANTI	Le amministrazioni e i gestori di pubblici servizi che detengono nei propri archivi le informazioni e i dati contenuti nelle dichiarazioni sostitutive, o richiesti direttamente dalle amministrazioni procedenti (*art. 1,comma 1, lett. p) del DPR n. 445/2000*);
AMMINISTRAZIONI PROCEDENTI	Le amministrazioni e, nei rapporti con l'utenza, i gestori di pubblici servizi che ricevono le dichiarazioni sostitutive ovvero provvedono agli accertamenti d'ufficio (art. 1, comma 1 lett. o) DPR n. 445/2000);
AMMINISTRAZIONI PUBBLICHE	Per amministrazioni pubbliche si intendono quelle indicate nell'art. 1, comma 2 del d.lgs. 30 marzo 2001, n. 165;
AMMINISTRAZIONI PUBBLICHE CENTRALI	Le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le istituzioni universitarie, gli enti pubblici non economici nazionali, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN), le agenzie di cui al decreto legislativo 30 luglio 1999, n. 300 (art. 1, comma 1 lett. z) del d.lgs. 7 marzo 2005, n. 82);
ARCHIVIO	L'archivio è la raccolta ordinata degli atti spediti, inviati o comunque formati dell'Amministrazione nell'esercizio delle funzioni attribuite per legge o regolamento, per il conseguimento dei propri fini istituzionali. Gli atti formati e/o ricevuti dall'Amministrazione o dalla Area Organizzativa omogenea sono collegati tra loro da un rapporto di interdipendenza, determinato dal procedimento o dall'affare al quale si riferiscono. Essi sono ordinati e conservati in modo coerente e accessibile alla consultazione; l'uso degli atti può essere amministrativo, legale o storico. L'archivio è unico, anche se, convenzionalmente, per motivi organizzativi, tecnici, funzionali e di responsabilità, l'archivio viene suddiviso in tre sezioni: corrente, di deposito e storica;
ARCHIVIO CORRENTE	Costituito dal complesso dei documenti relativi ad affari e a procedimenti amministrativi in corso di istruttoria e di trattazione o comunque verso i quali sussista un interesse attuale;
ARCHIVIO DI DEPOSITO	Costituito dal complesso dei documenti relativi ad affari e a procedimenti amministrativi conclusi, per i quali non risulta più necessaria una trattazione per il corrente svolgimento del procedimento amministrativo o comunque verso i quali sussista un interesse sporadico;
ARCHIVIO STORICO	Costituito da complessi di documenti relativi ad affari e a procedimenti amministrativi conclusi da oltre 40 anni e destinati, previa l'effettuazione delle operazioni di scarto, alla conservazione perenne;
AREA ORGANIZZATIVA OMOGENEA (AOO)	Un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445;
ASSEGNAZIONE	L'operazione d'individuazione dell'Ufficio Utente (UU) competente per la trattazione del procedimento amministrativo o affare, cui i documenti si riferiscono;

AUTENTICAZIONE DI SOTTOSCRIZIONE	L'attestazione, da parte di un pubblico ufficiale, che la sottoscrizione è stata apposta in sua presenza, previo accertamento dell'identità della persona che sottoscrive (art. 1,comma 1, lett. i) del DPR 28 dicembre 2000, n. 445);
AUTENTICAZIONE INFORMATICA	La validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne distinguono l'identità nei sistemi informativi, effettuata attraverso opportune tecnologie al fine di garantire la sicurezza dell'accesso; (art. 1, comma 1 lett. b) del d.lgs. 7 marzo 2005, n. 82);
BANCA DI DATI	Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti (art. 4 comma 1 lett. o) del d.lgs. 30 giugno 2003 n. 196);
BLOCCO	La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento (art. 4, comma 1, lett. d) del d.lgs. 30 giugno 2003 n. 196);
CARTA NAZIONALE DEI SERVIZI	Il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni (art. 1 comma1 lett. d) del d.lgs. 7 marzo 2005, n. 82);
CARTA D'IDENTITÀ ELETTRONICA	Il documento d'identità munito di fotografia del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità anagrafica del suo titolare (art. 1 comma 1, lett. c) del d.lgs. 7 marzo 2005, n. 82) ;
CASELLE DI POSTA ELETTRONICA ISTITUZIONALI	Le caselle di posta elettronica "ordinarie" e "certificate" (per le comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna) associate alle AOO delle amministrazioni, ai registri informatici di protocollo, agli altri registri e repertori informatici definiti nell'ambito dei sistemi di gestione documentale e protocollo informatico e utilizzate per lo scambio di messaggi tra AOO (Circolare n. 60/2013 dell'AgID);
CERTIFICATI ELETTRONICI	Gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità dei titolari stessi (art. 1, comma 1 lett. e) del d.lgs. 7 marzo 2005, n. 82);
CERTIFICATO QUALIFICATO	Il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva (art. 1 comma 1 lett.f) del d.lgs. 7 marzo 2005, n. 82);
CERTIFICATO	Il documento rilasciato da una amministrazione pubblica avente funzione di ricognizione, riproduzione o partecipazione a terzi di stati, qualità personali e fatti contenuti in albi, elenchi o registri pubblici o comunque accerta ti da soggetti titolari di funzioni pubbliche (art. 1 comma 1 lett. f) del DPR 28 dicembre 2000, n. 445);
CERTIFICATORE	Il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime (art. 1, comma 1 lett. g) del d.lgs. 7 marzo 2005, n. 82);
CLASSIFICAZIONE	L'operazione che consente di organizzare i documenti in relazione alle funzioni e alle modalità operative dell'Amministrazione.

COMUNICAZIONE	Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione (art. 4 comma 1 lett. l) del d.lgs. 30 giugno 2003 n. 196);
CONSERVAZIONE	L'insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione;
COPIA ANALOGICA DEL DOCUMENTO INFORMATICO	Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto (DPCM 13 novembre 2014 – allegato 1);
CREDENZIALI DI AUTENTICAZIONE	I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica (art. 4 comma 3 lett. d) del d.lgs. 30 giugno 2003 n. 196);
DATI GIUDIZIARI	I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del DPR 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale (art. 4, comma 1 lett. e) del d.lgs. 30 giugno 2003 n. 196);
DATI IDENTIFICATIVI	I dati personali che permettono l'identificazione diretta dell'interessato (art. 4, comma 1 lett. c) del d.lgs. 30 giugno 2003 n. 196);
DATI SENSIBILI	I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale (art. 4 comma 1, lett. ddd) del d.lgs. 30 giugno 2003 n. 196);
DATO ANONIMO	Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile (art. 4 comma 1 lett. n) del d.lgs. 30 giugno 2003 n. 196);
DATO PERSONALE	Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale (art. 4 comma 1 lett. b) del d.lgs. 30 giugno 2003 n. 196);
DATO PUBBLICO	Il dato conoscibile da chiunque (art. 1 comma 1 lett. n) del d.lgs. 7 marzo 2005, n. 82);
DATO A CONOSCIBILITA' LIMITATA	Il dato la cui conoscibilità è riservata per legge o regolamento a specifici soggetti o categorie di soggetti (art. 1 comma 1 lett. l) del d.lgs. 7 marzo 2005, n. 82);

DICHIARAZIONE SOSTITUTIVA DI ATTO DI NOTORIETA'	Il documento sottoscritto dall'interessato, concernente stati, qualità personali e fatti, che siano a diretta conoscenza di questi, resa nelle forme previste dall' art. 1 comma 1 lett. h) del DPR 28 dicembre 2000, n. 445;
DICHIARAZIONE SOSTITUTIVA DI CERTIFICAZIONE	Il documento, sottoscritto dall'interessato, prodotto in sostituzione del certificato (art. 1 comma 1 lett. g) del DPR 28 dicembre 2000, n. 445);
DIFFUSIONE	Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione (art. 4 del d.lgs. 30 giugno 2003 n. 196);
DOCUMENTO AMMINISTRATIVO	Ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa (art. 1 comma 1 lett. a) del DPR 28 dicembre 2000, n. 445);
DOCUMENTO ANALOGICO	La rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti (art. 1 comma 1 lett. p-bis) del d.lgs. 7 marzo 2005, n. 82);
DOCUMENTO DI RICONOSCIMENTO	Ogni documento munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica amministrazione italiana o di altri Stati, che consenta l'identificazione personale del titolare. (art. 1 comma 1 lett. c) del DPR 28 dicembre 2000, n. 445);
DOCUMENTO D'IDENTITA'	La carta d'identità ed ogni altro documento munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica amministrazione competente dello Stato italiano o di altri Stati, con la finalità prevalente di dimostrare l'identità personale del suo titolare (art. 1 comma 1 lett. d) del DPR 28 dicembre 2000, n. 445);
DOCUMENTO D'IDENTITA' ELETTRONICO	Il documento analogo alla carta d'identità elettronica rilasciato dal comune fino al compimento del quindicesimo anno di età (art. 1 comma 1 lett. e) del DPR 28 dicembre 2000, n. 445);
DOCUMENTO INFORMATICO	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1 comma 1 lett. p) del d.lgs. 7 marzo 2005, n. 82);
DOSSIER	È una aggregazione di più fascicoli che può essere costituita a seguito di esigenze operative dell'Amministrazione, come ad esempio, dossier riferiti ad un Ente o ad una persona che contengono fascicoli relativi a diversi procedimenti che riguardano lo stesso Ente o la stessa persona;
ESIBIZIONE	operazione che consente di visualizzare un documento conservato e di ottenerne copia (DPCM 13 novembre 2014 – allegato 1);
EVIDENZA INFORMATICA	Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica (DPCM 13 novembre 2014 – allegato 1);

FASCICOLAZIONE	L'operazione di riconduzione dei singoli documenti classificati in tanti fascicoli corrispondenti ad altrettanti affari o procedimenti amministrativi.
FASCICOLO	Insieme ordinato di documenti, che può fare riferimento ad uno stesso affare/procedimento/processo amministrativo, o ad una stessa materia, o ad una stessa tipologia documentaria, che si forma nel corso delle attività amministrative del soggetto produttore, allo scopo di riunire, a fini decisionali o informativi tutti i documenti utili allo svolgimento di tali attività. Nel fascicolo possono trovarsi inseriti documenti diversificati per formati, natura, contenuto giuridico, ecc., anche se è non è infrequente la creazione di fascicoli formati di insieme di documenti della stessa tipologia e forma raggruppati in base a criteri di natura diversa (cronologici, geografici, ecc.). I fascicoli costituiscono il tipo di unità archivistica più diffusa degli archivi contemporanei e sono costituiti, in base alle esigenze di servizio, secondo criteri che sono stabiliti per ciascuna voce del piano di classificazione al momento della sua elaborazione o del suo aggiornamento;
FIRMA DIGITALE	Un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici (art. 1 comma 1 lett. s) del d.lgs. 7 marzo 2005, n. 82);
FIRMA ELETTRONICA	L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica (art. 1, comma 1, lett. q) del d.lgs. 7 marzo 2005, n. 82);
FIRMA ELETTRONICA AVANZATA	L'insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati (art. 1 comma 1 lett. q-bis) del d.lgs. 7 marzo 2005, n. 82);
FIRMA ELETTRONICA QUALIFICATA	La firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica (art. 1 comma 1 lett. r) del d.lgs. 7 marzo 2005, n. 82);
FUNZIONE DI HASH	Una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti (DPCM 13 novembre 2014 – allegato 1);

GARANTE (della Privacy)	L'autorità di cui all'articolo 153 del d.lgs. 30 giugno 2003 n. 196, istituita dalla legge 31 dicembre 1996, n. 675 (art. 4 comma 1 lett. q) del d.lgs. 30 giugno 2003 n. 196);
GESTIONE INFORMATICA DEI DOCUMENTI	L'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici (art. 1 comma 1 lett. l) del d.lgs. 7 marzo 2005, n. 82);
IDENTIFICAZIONE INFORMATICA	La validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso informatici (art. 1 comma 1 lett. u-ter) del d.lgs. 7 marzo 2005, n. 82);
IMPRONTA	la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash (DPCM 13 novembre 2014 – allegato 1);
INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI	Le persone fisiche autorizzate a compiere operazioni di trattamento di dati personali dal titolare o dal responsabile;
INSERTO	È un sottoinsieme omogeneo del sottofascicolo che può essere costituito a seguito di esigenze operative dell'Amministrazione;
LEGALIZZAZIONE DI FIRMA	L'attestazione ufficiale della legale qualità di chi ha apposto la propria firma sopra atti, certificati, copie ed estratti, nonché dell'autenticità della firma stessa (art. 1 comma 1 lett. l) del DPR 28 dicembre 2000, n. 445);
LEGALIZZAZIONE DI FOTOGRAFIA	L'attestazione, da parte di una pubblica amministrazione competente, che un'immagine fotografica corrisponde alla persona dell'interessato (art. 1 comma 1 lett. n) del DPR 28 dicembre 2000, n. 445);
MASSIMARIO DI SELEZIONE E SCARTO DEI DOCUMENTI / PIANO DI CONSERVAZIONE	Il massimario di selezione e scarto è lo strumento che consente di effettuare razionalmente lo scarto archivistico dei documenti prodotti e ricevuti dalle pubbliche amministrazioni. Il massimario riproduce l'elenco delle partizioni e sottopartizioni del titolario con una descrizione più o meno dettagliata dei procedimenti/procedure attivate per le funzioni a cui ciascuna partizione si riferisce e della natura dei relativi documenti; indica per ciascun procedimento/ procedura, quali documenti debbano essere conservati permanentemente (e quindi versati dopo quarant'anni dall'esaurimento degli affari nei competenti archivi di Stato per gli uffici dello Stato o per la sezione degli archivi storici per gli Enti pubblici) e quali invece possono essere destinati al macero dopo cinque anni, dopo dieci anni, dopo venti anni, ecc. o secondo le esigenze dell'Amministrazione/AOO. Ne consegue il PIANO DI CONSERVAZIONE periodica o permanente dei documenti, nel rispetto delle vigenti disposizioni in materia di tutela dei beni culturali;

MEMORIZZAZIONE	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici (DPCM 13 novembre 2014 – allegato 1);
MISURE MINIME DI SICUREZZA	Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31 del d.lgs. 30 giugno 2003 n. 196 (art. 4 comma 3 lett. a) del d.lgs. 30 giugno 2003 n. 196);
PAROLA CHIAVE	Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica (art. 4, comma 3, lett. e) del d.lgs. 30 giugno 2003, n. 196);
ORIGINALI NON UNICI	I documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi (art. 1, comma 1, lett. v) del d.lgs. 7 marzo 2005, n. 82);
PIANO DI CONSERVAZIONE DEGLI ARCHIVI	Vedi MASSIMARO DI SELEZIONE E SCARTO
PROFILO DI AUTORIZZAZIONE	L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti (art. 4, comma 3, lett. f) del d.lgs. 30 giugno 2003 n. 196);
PROCESSO DI CONSERVAZIONE	L'insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 10 delle regole tecniche del sistema di conservazione (DPCM 13 novembre 2014 – allegato 1);
RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali (art. 4, comma 1, lett. g) del d.lgs. 30 giugno 2003 n. 196);
RESPONSABILE DEL SERVIZIO PER LA GESTIONE INFORMATICA DEI DOCUMENTI, DEI FLUSSI DOCUMENTALI E DEGLI ARTICOLI	Il responsabile del Servizio per la gestione informatica dei documenti, dei flussi documentali e degli archivi di cui all'articolo 61 (R) del DPR 28 dicembre 2000, n. 445;
RESPONSABILI DEI PROCEDIMENTI AMMINISTRATIVI **(RPA)**	È la persona, alla quale è stata affidata la trattazione di un affare amministrativo ivi compresa la gestione/creazione del relativo fascicolo dell'archivio corrente;
RIFERIMENTO TEMPORALE	Informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici (art 1, comma 1, lett. g) del DPCM 13 gennaio 2004) o ad un messaggio di posta elettronica certificata (art. 1, comma 1, lett. i), del DPR 11 febbraio 2005, n. 68);

SCOPI SCIENTIFICI	Le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore (art. 4, comma 4, lett. c) del d.lgs. 30 giugno 2003 n. 196);
SCOPI STATISTICI	Le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici (art. 4, comma 4, lett. b) del d.lgs. 30 giugno 2003 n. 196);
SCOPI STORICI	Le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato (art. 4, comma 4, lett. a) del d.lgs. 30 giugno 2003 n. 196);
SEGNATURA INFORMATICA	L'insieme delle informazioni che compongono la segnatura di protocollo sotto forma di documento XML da includere in un messaggio protocollato (Circolare n. 60/2013 dell'AgID);
SEGNATURA DI PROTOCOLLO	L'apposizione o l'associazione, all'originale del documento, in forma permanente e non modificabile delle informazioni riguardanti il documento stesso (Glossario dell'IPA Indice delle Pubbliche Amministrazioni);
SISTEMA DI CLASSIFICAZIONE	Strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata (DPCM 13 novembre 2014 – allegato 1);
SISTEMA DI CONSERVAZIONE	sistema di conservazione dei documenti informatici di cui all'articolo 44 del Codice (DPCM 13 novembre 2014 – allegato 1);
SISTEMA DI AUTORIZZAZIONE	L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente (art. 4, comma 3, lett. g) del d.lgs. 30 giugno 2003 n. 196);
SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI	L'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti (art. 1, comma 1, lett. r) del DPR 28 dicembre 2000 n. 445);
STRUMENTI ELETTRONICI	Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento di dati(art. 4, comma 3, lett. b) del d.lgs. 30 giugno 2003 n. 196).

Allegato 2

NORMATIVA DI RIFERIMENTO

1. **Legge 7 agosto 1990, n. 241** - Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi (G.U. del 18 agosto 1990, n. 192)
2. **DPR 27 giugno 1992, n. 352** - Regolamento per la disciplina delle modalità di esercizio e dei casi di esclusione del diritto di accesso ai documenti amministrativi, in attuazione dell'art. 24, comma 2, della Legge 7 agosto 1990, n. 241, recante nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi (G.U. 29 luglio 1992, n. 177)
3. **DPR 12 febbraio 1993, n. 39** - Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, a norma dell'art. 2, comma 1, lettera m), della legge 23 ottobre 1992, n. 421 (G.U. 10 febbraio 1993, n. 42)
4. **Legge 15 marzo 1997, n. 59** - Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della pubblica amministrazione e per la semplificazione amministrativa
5. **DPCM 28 ottobre 1999** - Gestione informatica dei flussi documentali nelle pubbliche amministrazioni. (G.U. 11 dicembre 1999, n. 290)
6. **Decreto legislativo 29 ottobre 1999, n. 490** - Testo unico delle disposizioni legislative in materia di beni culturali e ambientali, a norma dell'articolo 1 della legge 8 ottobre 1997, n. 352. (G.U. 27 dicembre 1999, n. 302)
7. **DPR 28 dicembre 2000, n. 445** - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa. (G.U. 20 febbraio 2001, n. 42)
8. **Decreto legislativo 30 marzo 2001, n. 165** - "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche"
9. **Direttiva del Ministro per la funzione pubblica del 13 dicembre 2001** – Formazione del personale. (G.U. del 31 gennaio 2002, n. 26)
10. **Direttiva 16 gennaio 2002, Dipartimento per l'innovazione e le tecnologie** – Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni statali
11. **Direttiva del Ministro per l'innovazione e le tecnologie, 9 dicembre 2002** – Trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali
12. **Direttiva del Ministro per l'innovazione e le tecnologie, 20 dicembre 2002** – Linee guida in materia di digitalizzazione dell'amministrazione
13. **Legge 27 dicembre 2002, n. 289** - Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato
14. **DPR 7 aprile 2003, n. 137** - Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del decreto legislativo 23 gennaio 2002
15. **Decreto legislativo 30 giugno 2003, n. 196** - Codice in materia di protezione dei dati personali
16. **Decreto Ministeriale 14 ottobre 2003** - Approvazione delle linee guida per l'adozione del protocollo informatico e per il trattamento informatico dei procedimenti amministrativi. (G.U. del 25 ottobre 2003, n. 249)

17. **Direttiva del Ministro per l'innovazione e le tecnologie 27 novembre 2003** - Impiego della posta elettronica nelle pubbliche amministrazioni (G.U. 12 gennaio 2004, n. 8)
18. **Direttiva 1999/93/CE** del Parlamento europeo e del consiglio del 13 dicembre 2003
19. **Direttiva 18 dicembre 2003** - Linee guida in materia di digitalizzazione dell'amministrazione per l'anno 2004. (G.U. 4 aprile 2004, n. 28)
20. **Decreto legislativo 22 gennaio 2004, n. 42** - Codice dei beni culturali e del paesaggio, ai sensi dell'art. 10 della legge 6 luglio 2002, n. 137 (G.U. 24 febbraio 2004, n. 28)
21. **Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68** - Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3. (GU 28 aprile 2005 n.97)
22. **Decreto legislativo 7 marzo 2005, n. 82** - Codice dell'amministrazione digitale (G.U. 16 maggio 2005 - Suppl. Ordinario n. 93)
23. **Decreto della Presidenza del Consiglio dei Ministri 10 febbraio 2010** - Fissazione del termine che autorizza l'autocertificazione circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza (G.U. 28 Aprile 2010 n. 98)
24. **Decreto legislativo 30 dicembre 2010, n. 235** - Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69. (G.U. 10 gennaio 2011 n. 6 - Suppl. Ordinario n. 8)
25. **Decreto della Presidenza del Consiglio dei Ministri 19 luglio 2012** - Definizione dei termini di validità delle autocertificazioni circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza di cui al decreto del Presidente del Consiglio dei Ministri 30 ottobre 2003, e dei termini per la sostituzione dei dispositivi automatici di firma (G.U. 10 ottobre 2012 n. 237)
26. **Circolare dell'Agenzia per l'Italia Digitale 23 gennaio 2013, n. 60 -** Formato e definizioni dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le pubbliche amministrazioni
27. **Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 -** Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71 (G.U. 21 maggio 2013, n. 117)
28. **Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013** - Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis , 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 (G.U. 12 marzo 2014, n. 59 - Suppl. Ordinario n. 20)
29. **Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013** - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 -bis , 23 -ter , comma 4, 43, commi 1 e 3, 44 , 44 -bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 (G.U. 12 marzo 2014, n. 59 - Suppl. Ordinario n.20)
30. **Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014** - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 (G.U. 12 gennaio 2015, n. 8)
31. **Circolare 18 aprile 2017**, n. 2/2017 dell'Agenzia per l'Italia Digitale, recante le misure minime di sicurezza ICT per le pubbliche amministrazioni;

32. **Circolare n. 2 del 9 aprile 2018**, recante i criteri per la qualificazione dei Cloud Service Provider per la PA;
33. **Circolare n. 3 del 9 aprile 2018**, recante i criteri per la qualificazione di servizi SaaS per il Cloud della PA;
34. **Reg. UE 2018/1807**, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea;
35. **DPCM 19 giugno 2019, n. 76**, Regolamento di organizzazione del Ministero per i beni e le attività culturali, degli uffici di diretta collaborazione del Ministro e dell'Organismo indipendente di valutazione della performance.

REGOLAMENTI COMUNALI

1. **Regolamento per il trattamento dei dati sensibili e** giudiziari - approvato con delibera di Consiglio Comunale n. 98 / 19.12.2005
2. **Regolamento per la disciplina dell'accesso ai documenti amministrativi** - approvato con delibera Consiglio Comunale n. 16 / 21.02.2008
3. **Regolamento disciplinante il procedimento amministrativo** - approvato con delibera Consiglio Comunale n. 79 / 19.12.1997
4. **Regolamento per l'esercizio del diritto di accesso da parte dei consiglieri comunali** - approvato con delibera Consiglio Comunale n. 138 / 09.12.2008
5. **Regolamento per la disciplina dell'Albo pretorio on-line** - approvato con delibera della Giunta Comunale n. 2 / 11.01.2011

Allegato 3

AREE ORGANIZZATIVE OMOGENEE E MODELLO ORGANIZZATIVO

Con delibera di Giunta n. 36 del 31 marzo 2015 è stata individuata un'unica Area Organizzativa Omogenea afferente ad un unico sistema di gestione documentale.

1. CARATTERIZZAZIONE DELL'AMMINISTRAZIONE

Denominazione dell'Amministrazione	COMUNE DI CASTELLETTO STURA
Codice fiscale	81000470039
Indirizzo completo della sede principale dell'Amministrazione a cui indirizzare l'eventuale corrispondenza convenzionale	Via MUNICIPIO 1 12040 Castelletto Stura (CN)
Aree organizzative omogenee (AOO)	Unica
Denominazione dell'Area Organizzativa Omogenea	Protocollo Generale
Codice identificativo assegnato alla AOOO	c_c165
Nominativo del responsabile della gestione documentale	Dott. XXX
Caselle di posta elettronica istituzionali	PEC info@comune.castellettostura.cn.it. info@pec.comune.castellettostura.cn.it
Indirizzo completo della sede principale dell'AOO a cui indirizzare l'eventuale corrispondenza convenzionale	Via MUNICIPIO 1 12040 Castelletto Stura (CN)
Referente	

2. ARTICOLAZIONE DELLA AOO IN UNITA' ORGANIZZATIVE DI REGISTRAZIONE DEL PROTOCOLLO (UOP)

SETTORE	**DESCRIZIONE UOP**	**TIPO PROTOCOLLAZIONE:** ***<INGRESSO/USCITA>*** ***< INGRESSO >*** ***< USCITA >***
Settore 1°	ASSICURAZIONI	*Uscita*
	CENTRALINO	*Ingresso/Uscita*
	CONTRATTI	*Uscita*
	ECONOMATO E SERVIZI CIMITERIALI	*Uscita*
	ELETTORALE	*Ingresso/Uscita*
	GESTIONE RISORSE FINANZIARIE E ASSICURAZIONI	*Uscita*
	LEGALE	*Uscita*
	MESSI	*Uscita*
	PROTOCOLLO	*Ingresso/Uscita*
	RAGIONERIA	*Uscita*
	SEGRETERIA E UFFICIO DEL SINDACO	*Ingresso/Uscita*
	SISTEMI INFORMATICI	*Uscita* *Ingresso (solo per emergenze)*
	TRIBUTI	*Uscita*
Settore 2°	EDIFICI PUBBLICI	*Uscita*
	FUNZIONARIO TECNICO	*Uscita*
	PATRIMONIO E DEMANIO	*Uscita*
	POLIZIA AMMINISTRATIVA E COMMERCIO	*Uscita*
	SERVIZI DEMOGRAFICI	*Ingresso/Uscita*
	SERVIZI TECNICI, OPERE ED INFRASTRUTTURE (ufficio di staff)	*Uscita*
	SERVIZI URBANISTICI ED ISPETTIVI (ufficio di staff)	*Uscita*
	SUAP	*Ingresso/Uscita*
	VERDE PUBBLICO - AMBIENTE	*Uscita*
	VIABILITA' E NETTEZZA URBANA	*Uscita*
Settore 3°	CULTURA SPORT TURISMO ISTRUZ.	*Uscita*
	GESTIONE RISORSE UMANE INTERNE	*Uscita*
	SERVIZI ALLA PERSONA (ufficio di staff)	*Ingresso/Uscita*
POLIZIA LOCALE	POLIZIA LOCALE	*Uscita*

3. ARTICOLAZIONE DI CIASCUNA UNITA' ORGANIZZATIVA DI REGISTRAZIONE DI PROTOCOLLO (UOP) IN UFFICI UTENTE (UU)

Solo alcune UOP sono articolate in UU ossia svolgono attività di protocollazione per conto di altri uffici:

UOP	TIPO DI PROTOCOLLAZIONE	UU
PROTOCOLLO	*Ingresso*	- TUTTI GLI UFFICI COMUNALI (anche se alcuni uffici sono abilitati a protocollare in ingresso)
SERVIZI TECNICI, OPERE ED INFRASTRUTTURE (ufficio di staff)	*Uscita*	- TELECOMUNICAZIONI
SERVIZI URBANISTICI ED ISPETTIVI (ufficio di staff)	*Uscita*	- EDILIZIA PRIVATA - STRUMENTI ESECUTIVI E VIGILANZA
SERVIZI ALLA PERSONA (ufficio di staff)	*Uscita*	- ASILO NIDO - CENTRO DIURNO - SERVIZI DI SOSTEGNO ADULTI - SERVIZI DI SOSTEGNO ANZIANI - SERVIZI DI SOSTEGNO MINORI - SPORTELLI
	Ingresso (posta riservata)	- SERVIZI DI SOSTEGNO ADULTI - SERVIZI DI SOSTEGNO ANZIANI - SERVIZI DI SOSTEGNO MINORI

4. ARTICOLAZIONE DELL'AMMINISTRAZIONE IN UOR/UU

La struttura organizzativa del Comune si articola in Settori, Servizi, Uffici ed è così articolata:

SETTORE	SERVIZIO	UFFICI
Settore I **Gestione e Sviluppo Risorse** DIRIGENTE: Dr. Corrado Zanetta	SEGRETERIA GENERALE - U.R.P. - UFFICIO DEL SINDACO, PROTOCOLLO, MESSI E CENTRALINO	*Segreteria e ufficio del Sindaco*
		Protocollo, Messi, Centralino
		URP
	LEGALE E CONTRATTI	*Legale*
		Contratti
	ELETTORALE	-
	SISTEMI INFORMATICI	-
	GESTIONE RISORSE FINANZIARIE, SERVIZI CIMITERIALI E ASSICURAZIONI Capo servizio: Dr.ssa Anna Bodio	*Ragioneria*
		Economato e Servizi cimiteriali
		Assicurazioni
	TRIBUTI Capo servizio: Rag. Maurizio Luongo	-
Settore II **Servizi per il Territorio** DIRIGENTE: Ing. Mauro Marchisio	**SERVIZI URBANISTICI ED ISPETTIVI** Capo servizio: Arch. Alberto Clerici	*Edilizia Privata*
		Strumenti esecutivi e vigilanza
	SERVIZI TECNICI, OPERE ED INFRASTRUTTURE	*Funzionario Tecnico* - *Edifici pubblici* - *Viabilità e nettezza urbana*
		Verde Pubblico - Ambiente
		Telecomunicazioni
	PATRIMONIO E DEMANIO	-
	SERVIZIO DI POLIZIA AMMINISTRATIVA, COMMERCIO E SERVIZI DEMOGRAFICI Capo servizio: Dr.ssa Monica Rondoni	*Polizia Amministrativa, e Commercio*
		Servizi Demografici
	SPORTELLO UNICO ATTIVITÀ PRODUTTIVE Capo servizi: Arch. Alberto Clerici e Dr.ssa Monica Rondoni	-
Settore III **Servizi alla Persona e Gestione risorse umane interne** DIRIGENTE: Dr. Giovanni Vesco	SERVIZI SOCIO ASSISTENZIALI EDUCATIVI	*Asilo Nido*
		Centro Diurno
		Segretariato sociale e sportelli
		Servizi di sostegno Adulti
		Servizi di sostegno Anziani
		Servizi di sostegno Minori
		Sportelli
	GESTIONE RISORSE UMANE INTERNE	-
	GESTIONE DEI RAPPORTI ECONOMICI CON LE ASSOCIAZIONI	-
	ISTRUZIONE, CULTURA, SPORT E TURISMO Capo Servizio: Dr.ssa Nadia Pirali	*Biblioteca*
		Sport e turismo
		Istruzione
		Scuolabus
	SERVIZIO DI POLIZIA LOCALE Capo Servizio: Dr.ssa Donatella Creuso	*Ispettivo amministrativo*
		Ufficio di Vigilanza
		Spettacoli viaggianti

5. UOR DESTINATARI DELLO SMISTAMENTO DEI DOCUMENTI RICEVUTI DALL'AOO E PROTOCOLLATI DALL'UFFICIO PROTOCOLLO GENERALE

SETTORE	UOR	UFFICI	ASSEGNAZIONE DOCUMENTI S/N
Settore I **Gestione e Sviluppo Risorse** DIRIGENTE: Dr. Corrado Zanetta	SEGRETERIA E UFFICIO DEL SINDACO Nel programma del protocollo più semplicemente "SEGRETERIA"		**N**
	MESSI		**N**
	CONTRATTI		**N**
	LEGALE		**N**
	ELETTORALE		**N**
	SISTEMI INFORMATICI		**N**
	GESTIONE RISORSE FINANZIARIE, SERVIZI CIMITERIALI E ASSICURAZIONI Nel programma del protocollo più semplicemente "SERVIZI FINANZIARI"	*Ragioneria* *Economato e Servizi cimiteriali* *Assicurazioni*	**S**
	TRIBUTI		**N**
Settore II **Servizi per il Territorio** DIRIGENTE: Ing. Mauro Marchisio	**SERVIZI URBANISTICI ED ISPETTIVI** Nel programma del protocollo più semplicemente "URBANISTICA"	*Edilizia Privata* *Strumenti esecutivi e vigilanza*	**N**
	SERVIZI TECNICI, OPERE ED INFRASTRUTTURE Nel programma del protocollo più semplicemente "LAVORI PUBBLICI (Servizi tecnici)"	*Funzionario Tecnico* *Edifici pubblici* *Viabilità e nettezza urbana*	**S**
	AMBIENTE		**N**
	TELECOMUNICAZIONI		**N**
	PATRIMONIO E DEMANIO Nel programma del protocollo più semplicemente "PATRIMONIO"		**N**
	POLIZIA AMMINISTRATIVA, COMMERCIO E SERVIZI DEMOGRAFICI Nel programma del protocollo più semplicemente "POLIZIA AMMINISTRATIVA"		**N**
	SERVIZI DEMOGRAFICI Nel programma del protocollo più semplicemente "DEMOGRAFICI"		**N**
	SPORTELLO UNICO ATTIVITÀ PRODUTTIVE Nel programma del protocollo più semplicemente "SUAP"		**N**

Settore III **Servizi alla Persona e Gestione risorse Umane interne** DIRIGENTE: Dr. Giovanni Vesco	SEGR. 3° SETTORE - SERVIZI ALLA PERSONA	*Asilo Nido*	**S**
		Centro Diurno	
		Segretariato sociale e sportelli	
		Servizi di sostegno Adulti	
		Servizi di sostegno Anziani	
		Servizi di sostegno Minori	
		Sportelli	
		Gestione dei rapporti economici con le associazioni	
	GESTIONE RISORSE UMANE INTERNE Nel programma del protocollo più semplicemente "PERSONALE"	-	**N**
	ISTRUZIONE, CULTURA, SPORT E TURISMO Capo Servizio: Dr.ssa Nadia Pirali	*Biblioteca*	**S**
		Sport e turismo	
		Istruzione	
		Scuolabus	
	SERVIZIO DI POLIZIA LOCALE Capo Servizio: Dr.ssa Donatella Creuso	*Ispettivo amministrativo*	**S**
		Ufficio di Vigilanza	
		Spettacoli viaggianti	

6. CODICI UNIVOCI UFFICI AI FINI DELL'EMISSIONE DELLE FATTURE ELETTRONICHE

ELENCO UFFICI	**CODICE UNIVOCO UFFICIO**
RAGIONERIA	NOWUZW

Allegato 4

ATTO DI NOMINA
DEL RESPONSABILE DELLA GESTIONE DOCUMENTALE

Decreto del Sindaco

N. 4 del 30/09/2025

Oggetto: Nomina responsabile della gestione documentale e della conservazione e del sostituto per i casi di vacanza, assenza o impedimento.

Richiamati:
- l'articolo 4, comma 1, lettera e), del decreto legislativo 30 marzo 2001 n. 165 e smi;
- l'articolo 50, comma 10, del decreto legislativo 18 agosto 2000, n. 267 che conferisce al Sindaco i poteri di nomina dei responsabili di uffici e servizi;
- l'articolo 97, comma 4, lettera d), del TUEL per il quale il Segretario Comunale *esercita ogni altra funzione attribuitagli dallo statuto o dai regolamenti, o conferitagli dal Sindaco o dal Presidente della Provincia*;
- l'articolo 7 comma 4 del DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 3 dicembre 2013 (Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 -bis , 23-ter , comma 4, 43, commi 1 e 3, 44 , 44 -bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005) per il quale *nelle pubbliche amministrazioni, il ruolo di responsabile della conservazione può essere svolto dal responsabile della gestione documentale*.

Premesso che:
- In attuazione dell'art. 61 del testo unico, le pubbliche amministrazioni di cui all'art. 2, comma 2, del Codice definiscono le attribuzioni del responsabile della gestione documentale, i cui compiti, come individuati dall'art. 4 del DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 3 dicembre 2013 (Regole tecniche per il protocollo informatico ai sensi degli articoli 40 -bis , 41, 47, 57 -bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005), sono i seguenti:
  a) predisporre lo schema del manuale di gestione di cui all'art. 5;
  b) proporre i tempi, le modalità e le misure organizzative e tecniche di cui all'art. 3, comma 1, lettera e);
  c) predisporre il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici nel rispetto delle misure minime di sicurezza previste nel disciplinare tecnico pubblicato in allegato B del decreto legislativo del 30 giugno 2003, n. 196 e successive modificazioni, d'intesa con il responsabile della conservazione, il responsabile dei sistemi informativi o, nel caso delle pubbliche amministrazioni centrali, il responsabile dell'ufficio di cui all'art. 17

del Codice e con il responsabile del trattamento dei dati personali di cui al suddetto decreto.

Premesso inoltre che:

- è necessario procedere anche alla nomina di un responsabile della conservazione, i cui compiti sono individuati dall'art. 7 del DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 3 dicembre 2013 (Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 -bis , 23-ter , comma 4, 43, commi 1 e 3, 44 , 44 -bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005) e in particolare:
  a) definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;
  b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
  c) genera il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
  d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
  e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
  f) assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
  g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
  h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
  i) adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12;
  j) assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
  k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per espletamento delle attività di verifica e di vigilanza;
  l) provvede, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti;
  m) predispone il manuale di conservazione di cui all'art. 8 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

DECRETA

1. dalla data odierna e sino alla scadenza del mandato elettorale, il Segretario Dr. Alessandro Rabino, iscritto all'Albo regionale del Piemonte è individuato quale:
   responsabile della gestione documentale e responsabile della conservazione;

2. dalla data odierna e sino alla scadenza del mandato elettorale, l'addetto al protocollo, sig.ra Rosaria Tufaro, è individuato quale suo vicario per i casi di vacanza, assenza o impedimento del primo.

F.to IL SINDACO
Alessandro Dacomo

Allegato 5

ELENCO DELLE PERSONE TITOLARI DI FIRMA DIGITALE

Nominativo	Titolo/Ruolo nell'AOO	Estremi e descrizione della delega ricevuta
Rabino dott. Alessandro	**SEGRETARIO COMUNALE**	
Revelli Gemma	**URBANISTICA - EDILIZIA PRIVATA**	
Parrino Agostina	**RAGIONERIA**	

Allegato 6

PIANO DI SICUREZZA DEI DOCUMENTI INFORMATICI

ASPETTI FONDAMENTALI DELLA SICUREZZA

Gli aspetti fondamentali del sistema di sicurezza sono:

- protezione fisica delle risorse
- protezione logica delle informazioni
- norme per il personale

PROTEZIONE FISICA DELLE RISORSE

L'obiettivo della protezione fisica delle risorse è quello di proteggere le aree e le componenti del sistema informativo.
Generalmente le contromisure di sicurezza fisica possono essere ricondotte a sicurezza di area e sicurezza delle apparecchiature.
La sicurezza di area ha il compito di prevenire accessi fisici non autorizzati, danni o interferenze con lo svolgimento dei servizi informatici. Le contromisure si riferiscono alle protezioni perimetrali dei siti, ai controlli fisici all'accesso, alla sicurezza delle sale computer rispetto a danneggiamenti accidentali o intenzionali, alla protezione fisica dei supporti.
La sicurezza delle apparecchiature e' riconducibile da un lato alle protezioni da danneggiamenti accidentali o intenzionali e dall'altro alla sicurezza degli impianti di alimentazione e di condizionamento. Anche la manutenzione dell'hardware rientra in questa area, come anche la protezione da manomissione o furti.
Le contromisure adottate sono le seguenti:

- I locali dove trovano alloggiamento i server sono chiusi a chiave, dotati di impianto di condizionamento e di sensori per il rilevamento di fumi.
- Le chiavi di accesso ai locali sono distribuite ai soli dipendenti dell'ufficio Sistemi Informatici ed ai servizi di sorveglianza.
- Le apparecchiature sono altresì protette da sbalzi di tensione elettrica tramite UPS dipartimentali.

PROTEZIONE LOGICA DELLE INFORMAZIONI

Gli obiettivi della protezione logica delle informazioni sono:

- il controllo degli accessi alle informazioni
- il mantenimento della loro integrità e riservatezza
- la sicurezza nella trasmissione e nelle comunicazioni all'interno dell'Amministrazione e con l'esterno (Internet, altre Amministrazioni etc..)
- la sicurezza delle stazioni di lavoro e dei personal computer
- la tempestiva rilevazione di eventuali incidenti di sicurezza.

Il campo di applicazione della Sicurezza Logica riguarda principalmente la protezione dell'informazione, e di conseguenza di dati, applicazioni, sistemi e reti, sia in relazione al loro corretto funzionamento ed utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo.
Le contromisure di Sicurezza Logica sono quindi da intendersi come l'insieme di misure di sicurezza di carattere tecnologico e di natura procedurale ed organizzativa che concorrono nella realizzazione del livello di sicurezza da raggiungere.
Le contromisure adottate sono le seguenti:

- Sistema operativo del PdP utilizzato dall'amministrazione, conforme alle specifiche previste dalla classe ITSEC F-C2/E2 o a quella C2 delle norme TCSEC e loro successive evoluzioni (scritture di sicurezza e controllo accessi);

- uso di sistemi RAID (si tratta di hard disk multipli visti però dal sistema operativo come un singolo disco. La principale proprietà di questi dispositivi è quella di garantire la disponibilità e l'integrità dei dati anche nel caso di guasto hardware di uno dei dischi;
- protezione dei sistemi di acceso e conservazione delle informazioni con assegnazione ad ogni utente del sistema di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- cambio delle password con frequenza almeno bi*mestrale* durante la fase di esercizio;
- sistemi di backup giornalieri;
- conservazione, a cura dell'ufficio Sistemi Informatici delle copie di riserva dei dati e dei documenti, in locali diversi e se possibile lontani da quelli in cui è installato il sistema di elaborazione di esercizio che ospita il PdP;
- firewall perimetrale che protegge la LAN da intrusioni esterne e web/mail server collocato in DMZ per non compromettere la sicurezza della LAN;
- server accessibili dall'esterno solo tramite vpn o tramite attivazione all'interno della LAN di software per il controllo remoto;
- software anti-virus, con gestione centralizzata, su ogni PC e server;
- manutenzione dei gestionali in uso e gestione dei "moduli" (patch e service pack) correttivi dei sistemi operativi;
- gestione delle situazioni di emergenza informatica attraverso la costituzione di un gruppo costituito dal personale in dotazione all'ufficio Sistemi Informatici e da risorse esterne qualificate;
- Piano di Continuità Operativa necessario a garantire la continuità del servizio informatico e la disponibilità delle informazioni (aggiornate), evitando o limitando i danni al patrimonio informativo a fronte di una emergenza. Il sistema informativo deve essere ripristinato entro sette giorni.

NORME PER IL PERSONALE

POLITICHE ACCETTABILI DI USO DEL SISTEMA INFORMATIVO

Premessa	E' necessario stabilire le regole per proteggere l'Amministrazione da azioni illegali o danneggiamenti effettuati da individui in modo consapevole o accidentale. Sono di proprietà dell'Amministrazione i sistemi di accesso ad Internet, l'Intranet, la Extranet ed i sistemi correlati, includendo in ciò anche i sistemi di elaborazione, la rete e gli apparati di rete, il software applicativo, i sistemi operativi, i sistemi di memorizzazione/archiviazione delle informazioni, il servizio di posta elettronica, i sistemi di accesso e navigazione in Internet, etc. Questi sistemi e/o servizi devono essere usati nel corso delle normali attività di ufficio solo per scopi istituzionali e nell'interesse dell'Amministrazione e in rapporto con possibili interlocutori della medesima. L'efficacia e l'efficienza della sicurezza è uno sforzo di squadra che coinvolge la partecipazione ed il supporto di tutto il personale (impiegati funzionari e dirigenti) dell'Amministrazione ed i loro interlocutori che vivono con l'informazione del sistema informativo. È responsabilità di tutti gli utilizzatori del sistema informatico conoscere queste linee guida e comportarsi in accordo con le medesime.
Scopo	Lo scopo di queste politiche è sottolineare l'uso accettabile del sistema informatico dell'Amministrazione. Le regole sono illustrate per proteggere gli impiegati e l'Amministrazione. L'uso non appropriato delle risorse strumentali espone l'Amministrazione al rischio di non poter svolgere i compiti istituzionali assegnati, a seguito, ad esempio, di virus, della compromissione di componenti del sistema informatico, ovvero di eventi disastrosi.
Ambito di applicazione	Queste politiche si applicano a tutti gli impiegati dell'Amministrazione e al personale esterno (interinali, stagisti, consulenti, ...) e a tutti gli apparati che sono di proprietà dell'Amministrazione o "affittate" da questa.

Politiche – Uso generale e proprietà

- Gli utenti del sistema informativo dovrebbero essere consapevoli che i dati da loro creati sui sistemi dell'Amministrazione e comunque trattati, rimangono di proprietà della medesima.
- Gli impiegati sono responsabili dell'uso corretto delle postazioni di lavoro assegnate e dei dati ivi conservati anche perché la gestione della rete (Intranet) non può garantire la confidenzialità dell'informazione memorizzata su ciascun componente "personale" della rete dato che l'amministratore della rete ha solo il compito di fornire prestazioni elevate e un ragionevole livello di confidenzialità e integrità dei dati in transito.
- Per garantire la manutenzione della sicurezza e della rete, soggetti autorizzati dall'Amministrazione (di norma amministratori di rete) possono monitorare gli apparati, i sistemi ed il traffico in rete in ogni momento.

Politiche - Sicurezza e proprietà dell'informazione

- Il personale dell'Amministrazione dovrebbe porre particolare attenzione in tutti i momenti in cui ha luogo un trattamento delle informazioni per prevenire accessi non autorizzati alle informazioni.
- Mantenere le credenziali di accesso (normalmente UserID e password) in modo sicuro e non condividerle con nessuno. Gli utenti autorizzati ad utilizzare il sistema informativo sono responsabili dell'uso delle proprie credenziali, componente pubblica (UserID) e privata (password). Le password dovrebbero essere cambiate con il primo accesso al sistema informativo e successivamente, al minimo ogni quattro mesi, ad eccezione di coloro che trattano dati personali sensibili o giudiziari per i quali il periodo si riduce a tre mesi.
- Tutte le postazioni di lavoro (PC da tavolo e portatili) dovrebbero essere rese inaccessibili a terzi quando non utilizzate dai titolari per un periodo massimo di dieci minuti attraverso l'attivazione automatica del salva schermo protetto da password o la messa in stand-by con un comando specifico.
- Poiché le informazioni archiviate nei PC portatili sono particolarmente vulnerabili su essi dovrebbero essere esercitate particolari attenzioni.
- Eventuali attività di scambio di opinioni del personale dell'Amministrazione all'interno di "new group" che utilizzano il sistema di posta elettronica dell'Amministrazione dovrebbero contenere una dichiarazione che affermi che le opinioni sono strettamente personali e non dell'Amministrazione a meno che non si tratti di discussioni inerenti e di interesse dell'Amministrazione eseguite per conto della medesima.
- Tutti i PC, i server ed i sistemi di elaborazione in genere, che sono connessi in rete interna dell'Amministrazione (Intranet) e/o esterna (Internet/Extranet) di proprietà dell'Amministrazione o del personale, devono essere dotati di un sistema antivirus approvato dal responsabile della sicurezza dell'Amministrazione ed aggiornato.
- Il personale deve usare la massima attenzione nell'apertura dei file allegati alla posta elettronica ricevuta da sconosciuti perché possono contenere virus, bombe logiche e cavalli di Troia.
- Non permettete ai colleghi, né tanto meno ad esterni, di operare sulla vostra postazione di lavoro con le vostre credenziali, in quanto risultate voiautori di qualunque azione.

POLITICHE - ANTIVIRUS

Premessa	I virus informatici costituiscono ancora oggi la causa principale di disservizio e di danno delle Amministrazioni. I danni causati dai virus all'Amministrazione, di tipo diretto o indiretto, tangibili o intangibili, secondo le ultime statistiche degli incidenti informatici, sono i più alti rispetto ai danni di ogni altra minaccia. I virus, come noto, riproducendosi autonomamente, possono generare altri messaggi contagiati capaci di infettare, contro la volontà del mittente, altri sistemi con conseguenze negative per il mittente in termini di criminalità informatica e tutela dei dati personali.
Scopo	Stabilire i requisiti che devono essere soddisfatti per collegare le risorse elaborative ad Internet/Intranet/Extranet dell'Amministrazione al fine di assicurare efficaci ed efficienti azioni preventive e consuntive contro i virus informatici.
Ambito di applicazione	Queste politiche riguardano tutte le apparecchiature di rete, di sistema ed utente (PC) collegate ad Internet/Intranet/Extranet. Tutto il personale dell'Amministrazione è tenuto a rispettare le politiche di seguito richiamate.

Politiche per le azioni preventive

- Deve essere sempre attivo su ciascuna postazione di lavoro un prodotto antivirus aggiornabile da un sito disponibile sulla Intranet dell'Amministrazione.
- Su ciascuna postazione deve essere sempre attiva la versione corrente e aggiornata con la più recente versione resa disponibile sul sito centralizzato.
- Non aprire mai file o macro ricevuti con messaggi dal mittente sconosciuto, sospetto, ovvero palesemente non di fiducia. Cancellare immediatamente tali oggetti sia dalla posta che dal cestino.
- Non aprire mai messaggi ricevuti in risposta a messaggi "probabilmente" mai inviati.
- Cancellare immediatamente ogni messaggio che invita a continuare la catena di messaggi, o messaggi spazzatura.
- Non scaricare mai messaggi da siti o sorgenti sospette.
- Evitate lo scambio diretto ed il riuso di supporti rimovibili (floppy disk, CD, DVD, tape, pen drive, etc.) con accesso in lettura e scrittura a meno che non sia espressamente formulato in alcune procedure dell'amministrazione e, anche in questo caso, verificare prima la bontà del supporto con un antivirus.
- Evitare l'uso di software gratuito (freeware o shareware) o documenti di testo prelevati da siti Internet o copiato dai CD/DVD in allegato a riviste.
- Evitare l'utilizzo, non controllato, di uno stesso computer da parte di più persone.
- Evitare collegamenti diretti ad Internet via modem.
- Non utilizzare il proprio supporto di archiviazione rimovibile su di un altro computer se non in condizione di protezione in scrittura.
- Se si utilizza una postazione di lavoro che necessita di un "bootstrap" da supporti di archiviazione rimovibili, usare questo protetto in scrittura.
- Non utilizzare i server di rete come stazioni di lavoro.

- Non aggiungere mai dati o file ai supporti di archiviazione rimovibili contenenti programmi originali.
- Effettuare una scansione della postazione di lavoro con l'antivirus prima di ricollegarla, per qualsiasi motivo (es, riparazione, prestito a colleghi o impiego esterno), alla Intranet dell'Organizzazione.

Di seguito vengono riportati ulteriori criteri da seguire per ridurre al minimo la possibilità di contrarre virus informatici e di prevenirne la diffusione, destinati a tutto il personale dell'Amministrazione ed, eventualmente, all'esterno.

- Tutti gli incaricati del trattamento dei dati devono assicurarsi che i computer di soggetti terzi, esterni, qualora interagiscano con il sistema informatico dell'Amministrazione, siano dotati di adeguate misure di protezione antivirus.
- Il personale delle ditte addette alla manutenzione dei supporti informatici deve usare solo supporti rimovibili preventivamente controllati e certificati singolarmente ogni volta.
- I supporti di archiviazione rimovibili provenienti dall'esterno devono essere sottoposti a verifica da attuare con una postazione di lavoro dedicata, non collegata in rete (macchina da quarantena).
- Il personale deve essere a conoscenza che la creazione e la diffusione, anche accidentale dei virus è punita dall'Articolo 615 quinquies del Codice penale concernente la "Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico … [omissis]… che prevede la reclusione sino a due anni e la multa sino a lire venti milioni".
- Il software acquisito deve essere sempre controllato contro i virus e verificato perché sia di uso sicuro prima che sia installato.
- È proibito l'uso di qualsiasi software diverso da quello fornito dall'Amministrazione.
- In questo ambito, al fine di minimizzare i rischi di distruzione anche accidentale dei dati a causa dei virus informatici, il RSP stabilisce le protezioni software da adottare sulla base dell'evoluzione delle tecnologie disponibili sul mercato.

Politiche per le azioni consuntive

Nel caso in cui su una o più postazioni di lavoro dovesse verificarsi perdita di informazioni, integrità o confidenzialità delle stesse a causa di infezione o contagio da virus informatici, il titolare della postazione interessata deve immediatamente isolare il sistema e poi notificare l'evento al responsabile della sicurezza, o suo delegato, che deve procedere a:

- verificare se ci sono altri sistemi infettati con lo stesso Virus Informatico;
- verificare se il virus ha diffuso dati;
- identificare il virus;
- attivare l'antivirus adatto ad eliminare il virus rilevato e bonificare il sistema infetto;
- installare l'Antivirus adatto su tutti gli altri sistemi che ne sono sprovvisti;
- diffondere la notizia dell'evento, all'interno dell'Amministrazione, nelle forme opportune.

POLITICHE - USO NON ACCETTABILE DEL SISTEMA INFORMATIVO

Le seguenti attività sono in generale proibite. Il personale può essere esentato da queste restrizioni in funzione del ruolo ricoperto all'interno dell'Amministrazione (ad esempio, nessuno può disconnettere e/o disabilitare le risorse ad eccezione degli amministratori di sistema o di rete).
In nessun caso o circostanza il personale è autorizzato a compiere attività illegali utilizzando le risorse di proprietà dell'Amministrazione.
L'elenco seguente non vuole essere una lista esaustiva, ma un tentativo di fornire una struttura di riferimento per identificare attività illecite o comunque non accettabili.

Attività di rete e di sistema

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione:

- Violazioni dei diritti di proprietà intellettuale di persone o società, o diritti analoghi includendo, ma non limitando, l'installazione o la distribuzione di copie pirata o altri software prodotti che non sono espressamente licenziati per essere usati dall'Amministrazione.
- Copie non autorizzate di materiale protetto da copyright (diritto d'autore) includendo, ma non limitando, digitalizzazione e distribuzione di foto e immagini di riviste, libri, musica e ogni altro software tutelato per il quale l'Amministrazione o l'utente finale non ha una licenza attiva.
- È rigorosamente proibita l'esportazione di software, informazioni tecniche, tecnologia o software di cifratura, in violazione delle leggi nazionali ed internazionali.
- Introduzione di programmi maliziosi nella rete o nei sistemi dell'Amministrazione.
- Rivelazione delle credenziali personali ad altri o permettere ad altri l'uso delle credenziali personali, includendo in ciò i familiari o altri membri della famiglia quando il lavoro d'ufficio è fatto da casa o a casa.
- Usare un sistema dell'Amministrazione (PC o server) per acquisire o trasmettere materiale pedo-pornografico o che offende la morale o che è ostile alle leggi e regolamenti locali, nazionali o internazionali.
- Effettuare offerte fraudolente di prodotti, articoli o servizi originati da sistemi dell'Amministrazione con l'aggravante dell'uso di credenziali fornite dall'Amministrazione stessa.
- Effettuare affermazioni di garanzie, implicite o esplicite, a favore di terzi ad eccezione di quelle stabilite nell'ambito dei compiti assegnati.
- Realizzare brecce nelle difese periferiche della rete del sistema informativo dell'Amministrazione o distruzione della rete medesima, dove per brecce della sicurezza si intendono, in modo riduttivo:
    a) accessi illeciti ai dati per i quali non si è ricevuta regolare autorizzazione;
    b) attività di "sniffing";
    c) disturbo della trasmissione;
    d) spoofing dei pacchetti;
    e) negazione del servizio;
    f) le modifiche delle mappe di instradamento dei pacchetti per scopi illeciti;
    g) attività di scansione delle porte o del sistema di sicurezza è espressamente proibito salvo deroghe specifiche.
- Eseguire qualsiasi forma di monitor di rete per intercettare i dati in transito.
- Aggirare il sistema di autenticazione o di sicurezza della rete, dei server e delle applicazioni.

- Interferire o negare l'accesso ai servizi di ogni altro utente abilitato.
- Usare o scrivere qualunque programma o comando o messaggio che possa interferire o con i servizi dell'Amministrazione o disabilitare sessioni di lavoro avviate da altri utenti di Internet/Intranet/Extranet.
- Fornire informazioni o liste di impiegati a terze parti esterne all'Amministrazione.

Attività di messaggistica e comunicazione

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione:

- Inviare messaggi di posta elettronica non sollecitati, includendo "messaggi spazzatura", o altro materiale di avviso a persone che non hanno specificamente richiesto tale materiale (spamming).
- Ogni forma di molestia via e-mail o telefonica o con altri mezzi, linguaggio, durata, frequenza o dimensione del messaggio.
- Uso non autorizzato delle informazioni della testata delle e-mail,
- Sollecitare messaggi di risposta a ciascun messaggio inviato con l'intento di disturbare o collezionare copie.
- Uso di messaggi non sollecitati originati dalla Intranet per altri soggetti terzi per pubblicizzare servizi erogati dall'Amministrazione e fruibili via Intranet stessa.
- Invio di messaggi non legati alla missione dell'Amministrazione ad un grande numero di destinatari utenti di news group (news group spam).

POLITICHE PER L'INOLTRO AUTOMATICO DI MESSAGGI DI POSTA ELETTRONICA

Premessa	Lo scopo di queste politiche è prevenire rivelazioni non autorizzare o involontarie di informazioni confidenziali o sensitive dell'Amministrazione
Scopo	Lo scopo di queste politiche è prevenire rivelazioni non autorizzare o involontarie di informazioni confidenziali o sensitive dell'Amministrazione.
Ambito di applicazione	Queste politiche riguardano l'inoltro automatico di messaggi e quindi la possibile trasmissione involontaria di informazioni confidenziali o sensitive a tutti gli impiegati o soggetti terzi.

Politiche

Gli impiegati devono esercitare estrema attenzione quando inviano qualsiasi messaggio all'esterno dell'Amministrazione. A meno che non siano espressamente approvati dal Dirigente responsabile i messaggi non devono essere automaticamente inoltrati all'esterno dell'Amministrazione.

Informazioni confidenziali o sensitive non devono essere trasmesse per posta elettronica a meno che, non siano espressamente ammesse e precedentemente cifrate in accordo con il destinatario.

POLITICHE PER LE CONNESSIONI IN INGRESSO SU RETE COMMUTATA

Scopo	Proteggere le informazioni elettroniche dell'Amministrazione contro compromissione involontaria da parte di personale autorizzato ad accedere dall'esterno su rete commutata.
Ambito di applicazione	Lo scopo di queste politiche è definire adeguate modalità di accesso da remoto ed il loro uso da parte di personale autorizzato.

Politiche

Il personale dell'Amministrazione e le persone terze autorizzate possono utilizzare la linea commutata per guadagnare l'ingresso alla Intranet dell'Amministrazione. Tale accesso deve avvenire o tramite l'uso di VPN o tramite l'uso di sistemi di autenticazione forte quali per esempio password da usare una sola volta (one time password). È responsabilità del personale con i privilegi di accesso dall'esterno alla rete dell'Amministrazione garantire che personale non autorizzato possa accedere illecitamente alla Intranet dell'Amministrazione ed alle sue informazioni.

Tutto il personale che può accedere al sistema informativo dell'Amministrazione dall'esterno deve essere consapevole che tale accesso costituisce "realmente" una estensione del sistema informativo che potenzialmente può trasferire informazioni sensitive. Il personale e le persone terze devono, di conseguenza, porre in essere tutte le ragionevoli misure di sicurezza in loro possesso per proteggere il patrimonio informativo ed i beni dell'Amministrazione.

Solo la linea commutata convenzionale può essere utilizzata per realizzare il collegamento. Non sono ammessi cellulari per realizzare collegamenti dati facilmente intercettabili o che consentono un reinstradamento della connessione.

POLITICHE PER L'USO DELLA POSTA ISTITUZIONALE DELL'AMMINISTRAZIONE

Scopo	Evitare l'offuscamento dell'immagine dell'Amministrazione. Quando un messaggio di posta esce dall'Amministrazione il pubblico tenderà a vedere ed interpretare il messaggio come una affermazione ufficiale dell'Amministrazione.
Ambito di applicazione	La politica di seguito descritta intende illustrare l'uso appropriato della posta elettronica istituzionale in uscita che deve essere adottata da tutto il personale e dagli interlocutori dell'Amministrazione stessa..

Politiche – Usi proibiti

Il sistema di posta dell'Amministrazione non deve essere usato per la creazione o la distribuzione di ogni distruttivo od offensivo messaggio, includendo come offensivi i commenti su razza, genere, capelli, colore, disabilità, età, orientamenti sessuali, pornografia, opinioni e pratiche religiose o nazionalità. Gli impiegati che ricevono messaggi con questi contenuti da colleghi dovrebbero riportare questi eventi ai diretti superiori immediatamente.

Politiche – Uso personale

Non è ammesso l'uso della posta istituzionale per usi personali e, in ogni caso, non si deve dare seguito a catene di lettere o messaggi scherzosi, di disturbo o di altro genere.

POLITICHE PER LE COMUNICAZIONI WIRELESS

Scopo	Queste politiche proibiscono l'accesso alla rete dell'Amministrazione via rete wireless insicura. Solo i sistemi wireless che si adattano a queste politiche o hanno la garanzia di sicurezza certificata dal responsabile della sicurezza, possono essere utilizzati per realizzare i collegamenti all'Amministrazione.
Ambito di applicazione	La politica riguarda tutti i dispositivi di comunicazione dati senza fili collegati (PC e cellulari telefonici) alla Intranet dell'Amministrazione, ovvero qualunque dispositivo di comunicazione wireless capace di trasmettere "pacchetti" di dati. Dispositivi wireless e/o reti senza connettività alla Intranet dell'Amministrazione, sono esclusi da queste politiche.

Politiche

Tutti i "punti di accesso" o le "stazioni base" collegati alla Intranet devono essere registrati e approvati dal responsabile della sicurezza.

Questi dispositivi sono soggetti a periodiche "prove di penetrazione" e controlli (auditing).

Tutti i dispositivi di accesso alle LAN dell'Amministrazione devono utilizzare prodotti di venditori accreditati dal responsabile della sicurezza e configurati in sicurezza.

ASPETTI DI SICUREZZA INFORMATICA

PER LA FORMAZIONE, GESTIONE, TRASMISSIONE, INTERSCAMBIO, ACCESSO E CONSERVAZIONE DEI DOCUMENTI INFORMATICI

FORMAZIONE DEI DOCUMENTI

Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono:

- l'identificabilità del soggetto che ha formato il documento e l'amministrazione di riferimento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti all'interno della stessa AOO.

I documenti dell'AOO sono prodotti con l'ausilio di applicativi di videoscrittura o *text editor* che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura.
Si adottano preferibilmente i formati PDF, XML e TIFF. I documenti informatici prodotti dall'AOO con altri prodotti di *text editor* sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard (PDF, XML e TIFF) come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.

Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto con firma digitale.

Per attribuire una data certa a un documento informatico prodotto all'interno dell'AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui al decreto del Presidente del Consiglio dei Ministri del 13 novembre 2014 (Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.).

I documenti così formati, prima di essere inviati a qualunque altra stazione di lavoro interna all'AOO, sono sottoposti ad un controllo antivirus onde eliminare qualunque forma di contagio che possa arrecare danno diretto o indiretto all'amministrazione.

GESTIONE DEI DOCUMENTI

Il sistema di protocollo informatico assicura:

- l'univoca identificazione ed autenticazione degli utenti;
- la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
- la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificazione.

Il sistema di protocollo informatico consente:

- il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti.

- il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo (ad es. dati o transazioni) - presenti o transitate sul PdP - che è opportuno mantenere poiché possono essere necessarie sia in caso di controversie legali che abbiano ad oggetto le operazioni effettuate sul sistema stesso, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza.
Le registrazioni di sicurezza sono costituite:

- dai log di sistema generati dal sistema operativo;
- dai log dei dispositivi di protezione periferica del sistema informatico (firewall);
- dalle registrazioni del PdP.

I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultati solo in caso di necessità dal RGD e dal titolare dei dati e, ove previsto dalle forze dell'ordine.

TRASMISSIONE E INTERSCAMBIO DEI DOCUMENTI INFORMATICI

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche.
Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.
Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO o ad altre pubbliche amministrazioni, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.
Lo scambio per via telematica di messaggi protocollati tra AOO di amministrazioni diverse presenta, in generale, esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali, sensibili e/o giudiziari come previsto dal decreto legislativo del 30 giugno 2003, n. 196.

Scambio dei documenti all'esterno dell'amministrazione (interoperabilità dei sistemi di protocollo informatico

Per interoperabilità dei sistemi di protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare anche le attività ed i processi amministrativi conseguenti (articolo 55, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445).
Lo scambio dei documenti soggetti alla registrazione di protocollo è effettuato mediante messaggi di posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, o messaggi conformi ai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045 e 2049 e successive modificazioni.
Ogni messaggio protocollato deve riportare alcune informazioni archivistiche fondamentali, per facilitare il trattamento dei documenti da parte del ricevente. Tali informazioni sono incluse nella segnatura informatica di ciascun messaggio protocollato e sono codificate in formato XML.
Con provvedimento dell'Agenzia per l'Italia Digitale, vengono indicati le modalità di trasmissione dei documenti informatici, il tipo ed il formato delle informazioni archivistiche di protocollo minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni e associate ai messaggi protocollati.

Scambio dei documenti all'interno dell'amministrazione

Gli Uffici dell'amministrazione (UOR) si scambiano documenti informatici attraverso l'utilizzo delle caselle di posta elettronica in attuazione di quanto previsto dalla direttiva 27 novembre 2003 del Ministro per l'innovazione e le tecnologie concernente l' "impiego della posta elettronica nelle pubbliche amministrazioni".

ACCESSO AI DOCUMENTI INFORMATICI

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.
La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale.
Il PdP adottato dall'amministrazione:
• consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente;
• assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Accesso al registro di protocollo per utenti interni all'amministrazione

I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio.
Ciascun utente del PdP può accedere solamente ai documenti che sono stati assegnati al suo UOR, o agli Uffici Utente (UU) ad esso subordinati.
Un utente può avere la visibilità completa sul registro di protocollo solo a seguito di abilitazione.
Il personale dell'ufficio protocollo generale e dell'ufficio sistemi informatici sono abilitati alla visualizzazione completa sul registro protocollo.
Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'amministrazione. Nel caso in cui sia effettuata la registrazione di un documento riservato, la visibilità completa sul documento stesso è possibile solo alla persona destinataria del documento.
Di norma tutti gli utenti che devono protocollare sono abilitati alla consultazione, inserimento e modifica, ma è possibile abilitare un utente anche alla sola consultazione.
Solo il personale dell'ufficio Sistemi Informatici è invece abilitato all'annullamento.

CONSERVAZIONE DEI DOCUMENTI INFORMATICI

Per la conservazione dei documenti informatici si applicano le regole di cui al decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 (Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 -bis , 23 -ter , comma 4, 43, commi 1 e 3, 44 , 44 -bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.).

Ai sensi dell'art. 44 del Codice, la conservazione può essere svolta all'interno della struttura organizzativa del soggetto produttore dei documenti o affidandola, in modo totale o parziale, ad altri soggetti, pubblici o privati che offrono idonee garanzie organizzative e tecnologiche, anche accreditati come conservatori presso l'Agenzia per l'Italia digitale.
L'amministrazione ha optato per la seconda soluzione ed ha richiesto ed ottenuto, da parte della Soprintendenza Archivistica territorialmente competente, il nulla-osta preventivo alla sottoscrizione di un Accordo di collaborazione con il Servizio Polo Archivistico Regionale dell'Emilia-Romagna ai fini della conservazione dei documenti informatici su piattaforma digitale.

Per le modalità operative di trasmissione del contenuto del pacchetto di versamento al sistema di conservazione si rimanda al manuale di conservazione.

Il manuale di conservazione inoltre illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

Allegato 7

ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO

Sono esclusi dalla registrazione di protocollo tutti i documenti di cui all'art. 53 comma 5 del decreto del Presidente della Repubblica 20 dicembre 2000, n. 445:

- Gazzette ufficiali
- Bollettini ufficiali e notiziari della pubblica amministrazione
- Note di ricezione delle circolari e altre disposizioni
- Materiali statistici
- Atti preparatori interni
- Giornali e riviste
- Libri
- Materiali pubblicitari
- Inviti a manifestazioni
- Tutti i documenti già soggetti a registrazione particolare dell'amministrazione

Sono altresì esclusi dalla protocollazione, in ambito comunale, le seguenti tipologie documentarie:

- Offerte o preventivi di terzi non richiesti
- Biglietti d'occasione (condoglianze, auguri, congratulazioni, ringraziamenti ecc.)
- Allegati , se accompagnati da lettera di trasmissione
- Richieste ferie
- Richieste permessi
- Richieste di rimborso spese e missioni
- Ricevute di ritorno delle raccomandate A.R.
- Pubblicità conoscitiva di convegni /corsi di aggiornamento
- Convocazioni ad incontri o riunioni e corsi di formazione interni
- Certificati e affini
- Documenti che per loro natura non rivestono alcuna rilevanza giuridico-amministrativa presente o futura

I documenti che sono invece soggetti a particolare registrazione dell'Amministrazione e che, ai sensi dell'art. 53, com. 5 del DPR 445/2000, sono esclusi dalla protocollazione sono:

Area	Registrazione particolare	Modalità di trattamento
Affari istituzionali	Albo pretorio	Utilizzo applicazione software ad hoc
	Atti di organizzazione	Utilizzo applicazione software ad hoc
	Comunicazioni adozione delibere di Giunta	Utilizzo applicazione software ad hoc
	Contratti rogati dal Segretario generale	Utilizzo applicazione software ad hoc

	Contratti non rogati in forma pubblica dal Segretario generale	Utilizzo applicazione software ad hoc
	Decreti sindacali (repertorio atti)	Utilizzo applicazione software ad hoc
	Deliberazioni di Consiglio comunale (repertorio atti)	Utilizzo applicazione software ad hoc
	Deliberazioni di Giunta comunale (repertorio atti)	Utilizzo applicazione software ad hoc
	Direttive Assessori	
	Direttive Giunta Comunale	
	Ordinanze dirigenziali	Utilizzo applicazione software ad hoc
	Ordinanze sindacali	Utilizzo applicazione software ad hoc
	Notifiche	Utilizzo applicazione software ad hoc
	Verbali Consiglio comunale	Utilizzo applicazione software ad hoc
	Verbali Giunta comunale	Utilizzo applicazione software ad hoc
Ragioneria	Atti di liquidazione (registrazione informatica)	Utilizzo applicazione software ad hoc
	Fatture emesse(registrazione informatica)	Utilizzo applicazione software ad hoc
	Mandati di pagamento (registrazione informatica)	Utilizzo applicazione software ad hoc
	Registri IVA	Utilizzo applicazione software ad hoc
	Reversali di incasso (registrazione informatica)	Utilizzo applicazione software ad hoc
Demografici	Atti di stato civile (registrazione informatica)	Utilizzo applicazione software ad hoc
	Carte d'identità (registrazione informatica)	Utilizzo applicazione software ad hoc
	Certificati anagrafici	Utilizzo applicazione software ad hoc
	Pubblicazioni di matrimonio (registrazione informatica)	Utilizzo applicazione software ad hoc
	Tessere elettorali (registrazione informatica)	Utilizzo applicazione software ad hoc
Polizia Locale	Concessione contrassegno parcheggi invalidi	Fascicolazione annuale
	Documenti informatici ricevuti o inviati nell'ambito di sistemi dedicati allo scambio o alla consultazione di dati (ACI-PRA/MOTORIZZAZIONE)	

	Notizie di reato	Fascicolazione
	Rapporti incidenti (registrazione informatica)	Fascicolazione
	Verbali CdS (registrazione informatica)	Fascicolazione
	Verbali oggetti smarriti	Fascicolazione
	Verbali violazioni amministrative	Fascicolazione
	Registro veicoli rimossi	Fascicolazione

	Determinazioni di ordini di servizio inserite nei singoli fascicoli personali	Permanente	
	Ordini di servizio collettivi	Permanente	
	Autorizzazione allo svolgimento di incarichi esterni	2 anni	
5. Inquadramenti e applicazione contratti collettivi di lavoro			
	Criteri generali e normativa per gli inquadramenti e le applicazione dei contratti collettivi	Permanente	
	Determinazione dei ruoli e contratti collettivi	Permanente	NB i contratti con il singolo confluiscono nel
	Determinazioni relative ai singoli	Permanente	
6. Retribuzioni e compensi			
	Criteri generali e normativa per le retribuzioni e compensi	Permanente	
	Anagrafe delle prestazioni: schede	5 anni	
	Determinazioni inserite nei singoli fascicoli personali	5 anni dalla cessazione dal servizio	
	Ruoli degli stipendi: base di dati/ tabulati	Permanente	
	Provvedimenti giudiziari di requisizione dello stipendio	5 anni	
7. Trattamento fiscale, contributivo e assicurativo			
	Criteri generali e normativa per gli adempimenti fiscali, contributivi e assicurativi	Permanente	
	Trattamento assicurativo inserito nei singoli fascicoli personali	5 anni dalla chiusura del fascicolo	
	Trattamento contributivo inserito nei singoli fascicoli personali	5 anni dalla chiusura del fascicolo	
	Trattamento fiscale inserito nei singoli fascicoli personali	5 anni dalla chiusura del fascicolo	
	Assicurazione obbligatoria inserita nei singoli fascicoli personali	5 anni dalla chiusura del fascicolo	
8. Tutela della salute e sicurezza sul luogo di lavoro			
	Criteri generali e normativa per la tutela della salute e sicurezza sul luogo di lavoro	Permanente	
	Rilevazione dei rischi, ai sensi della 626/94: un fasc. per sede	Tenere l'ultima e scartare la precedente	
	Prevenzione infortuni	Permanente	
	Registro infortuni	Permanente	Per L. 626/94
	Verbali delle rappresentanze dei lavoratori per la sicurezza	Permanente	
	Denuncia di infortunio e pratica relativa, con referti, inserita nei singoli fascicoli personali	Permanente	
	Fascicoli relativi alle visite mediche ordinarie (medicina del lavoro)	10 anni	

Allegato 9

TITOLARIO DI CLASSIFICAZIONE

TITOLI

1 Amministrazione generale
2 Organi di governo, gestione, controllo, consulenza e garanzia
3 Risorse umane
4 Risorse finanziarie e patrimoniali
5 Affari legali
6 Pianificazione e gestione del territorio
7 Servizi alla persona
8 Attività economiche
9 Polizia locale e sicurezza pubblica
10 Tutela della salute
11 Servizi demografici
12 Elezioni e iniziative popolari
13 Affari militari
14 Oggetti diversi

CLASSI

TITOLO		CLASSE	
1	**Amministrazione generale**	1	Legislazione e circolari esplicative
		2	Denominazione, territorio e confini, circoscrizioni di decentramento , toponomastica
		3	Statuto
		4	Regolamenti
		5	Stemma, gonfalone, sigillo
		6	Archivio generale
		7	Sistema informativo
		8	Informazioni e relazioni con il pubblico
		9	Politica del personale; ordinamento degli uffici e dei servizi
		10	Relazioni con le organizzazioni sindacali e di rappresentanza del personale
		11	Controlli interni ed esterni
		12	Editoria e attività informativo-promozionale interna ed esterna
		13	Cerimoniale, attività di rappresentanza; onorificenze e riconoscimenti
		14	Interventi di carattere politico e umanitario; rapporti istituzionali
		15	Forme associative e partecipative per l'esercizio di funzioni e servizi e adesione del Comune ad Associazioni
		16	Area e città metropolitana

		17	Associazionismo e partecipazione
2	**Organi di governo, gestione, controllo, consulenza e garanzia**	1	Sindaco
		2	Vice-sindaco
		3	Consiglio
		4	Presidente del Consiglio
		5	Conferenza dei capigruppo e Commissioni del Consiglio
		6	Gruppi consiliari
		7	Giunta
		8	Commissario prefettizio e straordinario
		9	Segretario e Vice-segretario
		10	Direttore generali e dirigenza
		11	Revisori dei conti
		12	Difensore civico
		13	Commissario ad acta
		14	Organo di controllo interni
		15	Organi consultivi
		16	Consigli circoscrizionali
		17	Presidente dei Consigli circoscrizionali
		18	Organi esecutivi circoscrizionali
		19	Commissioni dei Consigli circcoscrizionali
		20	Segretari delle circoscrizioni
		21	Commissario ad acta delle circoscrizioni
		22	Conferenza dei Presidenti di quartiere
3	**Risorse umane**	1	Concorsi, selezioni, colloqui
		2	Assunzioni e cessazioni
		3	Comandi e distacchi; mobilità
		4	Attribuzione di funzioni, ordini di servizio e missioni
		5	Inquadramenti e applicazione contratti collettivi di lavoro
		6	Retribuzioni e compensi
		7	Trattamento fiscale, contributivo e assicurativo
		8	Tutela della salute e sicurezza sul luogo di lavoro
		9	Dichiarazioni di infermità ed equo indennizzo
		10	Indennità premio di servizio e trattamento di fine rapporto, quiescenza
		11	Servizi al personale su richiesta
		12	Orario di lavoro, presenze e assenze
		13	Giudizi, responsabilità e provvedimenti disciplinari
		14	Formazione e aggiornamento professionale
		15	Collaboratori esterni
4	**Risorse finanziarie e patrimoniali**	1	Bilancio preventivo e Piano esecutivo di gestione (PEG)
		2	Gestione del bilancio e del PEG (con eventuali

			variazioni)
		3	Gestione delle entrate: accertamento, riscossione, versamento
		4	Gestione della spesa: impegno, liquidazione, ordinazione e pagamento
		5	Partecipazioni finanziarie
		6	Rendiconto della gestione ; adempimenti e verifiche contabili
		7	Adempimenti fiscali, contributivi e assicurativi
		8	Beni immobili
		9	Beni mobili
		10	Economato
		11	Oggetti smarriti e recuperati
		12	Tesoreria
		13	Concessionari ed altri incaricati della riscossione delle entrate
		14	Pubblicità e pubbliche affissioni
5	**Affari legali**	1	Contenzioso
		2	Responsabilità civile e patrimoniale verso terzi; assicurazioni
		3	Pareri e consulenze
6	**Pianificazione e gestione del territorio**	1	Urbanistica : piano regolatore generale e varianti
		2	Urbanistica: strumenti di attuazione del Piano regolatore generale
		3	Edilizia privata
		4	Edilizia pubblica
		5	Opere pubbliche
		6	Catasto
		7	Viabilità
		8	Servizio idrico integrato , luce, gas, trasporti pubblici, gestione dei rifiuti e altri servizi
		9	Ambiente : autorizzazioni, monitoraggio e controllo
		10	Protezione civile ed emergenze
7	**Servizi alla persona**	1	Diritto allo studio e servizi
		2	Asili nido e scuola materna
		3	Promozione e sostegno delle istituzioni di istruzione e della loro attività
		4	Orientamento professionale ; educazione degli adulti ; mediazione culturale
		5	Istituti culturali (Musei, biblioteche, teatri, Scuola comunale di musica, etc.)
		6	Attività ed eventi culturali
		7	Attività ed eventi sportivi
		8	Pianificazione e accordi strategici con enti pubblici e privati e con il volontariato sociale
		9	Prevenzione, recupero e reintegrazione dei soggetti

			a rischio
		10	Informazione, consulenza ed educazione civica
		11	Tutela e curatela di incapaci
		12	Assistenza diretta e indiretta , benefici economici
		13	Attività ricreativa e di socializzazione
		14	Politiche per la casa
		15	Politiche per il sociale
8	**Attività economiche**	1	Agricoltura e pesca
		2	Artigianato
		3	Industria
		4	Commercio
		5	Fiere e mercati
		6	Esercizi turistici e strutture ricettive
		7	Promozione e servizi
		8	S.U.A.P.
9	**Polizia locale e sicurezza pubblica**	1	Prevenzione ed educazione stradale
		2	Polizia stradale
		3	Informative
		4	Sicurezza e ordine pubblico
10	**Tutela della salute**	1	Salute e igiene pubblica
		2	Trattamenti Sanitari Obbligatori
		3	Farmacie
		4	Zooprofilassi veterinaria
		5	Randagismo animale e ricoveri
11	**Servizi demografici**	1	Stato civile
		2	Anagrafe e certificazioni
		3	Censimenti
		4	Polizia mortuaria e cimiteri
12	**Elezioni e iniziative popolari**	1	Albi elettorali
		2	Liste elettorali
		3	Elezioni
		4	Referendum
		5	Istanze, petizioni e iniziative popolari
13	**Affari militari**	1	Leva e servizio civile sostitutivo
		2	Ruoli matricolari
		3	Caserme, alloggi e servitù militari
		4	Requisizioni per utilità militari

Allegato 10

REPERTORI GENERALI

TITOLO I – AMMINISTRAZIONE GENERALE

Classe		**Tipologie documentarie**
6	Archivio generale	Ordinanze del Sindaco (serie con repertorio)
		Decreti del Sindaco (serie con repertorio)
		Ordinanze dei dirigenti
		Determinazioni dei dirigenti
		Deliberazioni del Consiglio comunale
		Deliberazioni della Giunta comunale
		Verbali delle adunanze del Consiglio comunale
		Verbali delle adunanze della Giunta comunale
		Verbali degli altri organi collegiali del Comune
		Contratti e convenzioni
		Atti rogati dal segretario comunale (contratti e atti unilaterali in forma pubblica amministrativa)
		Registro di protocollo
		Repertorio dei fascicoli
		Registro dell'Albo pretorio
		Registro delle notifiche
17	Associazionismo e partecipazione	Albo dell'associazionismo: elenco delle associazioni accreditate

TITOLO III – RISORSE UMANE

Classe		**Tipologie documentarie**
8	Tutela della salute e sicurezza sul luogo di lavoro	Registro infortuni
		Verbali dei rappresentanti dei lavoratori per la sicurezza
15	Collaboratori esterni	Elenco degli incarichi conferiti

TITOLO IV – RISORSE FINANZIARIE E PATRIMONIALI

Classe		**Tipologie documentarie**
3	Gestione delle entrate: accertamento, riscossione, versamento	Fatture emesse
		Reversali
4	Gestione della spesa: impegno, liquidazione, ordinazione e pagamento	Atti di liquidazione
		Mandati
8	Beni immobili	Concessioni di occupazione di spazi e aree pubbliche
		Concessioni di beni del demanio statale
		Concessioni cimiteriali

TITOLO VI – PIANIFICAZIONE E GESTIONE DEL TERRITORIO

Classe		**Tipologie documentarie**
3	Edilizia privata	Concessioni edilizie

TITOLO VIII – ATTIVITÀ ECONOMICHE

Classe		**Tipologie documentarie**
2	Artigianato	Autorizzazioni artigiane
4	Commercio	Autorizzazioni commerciali
6	Esercizi turistici e strutture ricettive	Autorizzazioni turistiche

TITOLO IX – POLIZIA LOCALE E SICUREZZA PUBBLICA

Classe		**Tipologie documentarie**
2	Polizia stradale	Verbali di accertamento di violazioni al Codice della strada
		Verbali di rilevazione incidenti
4	Sicurezza e ordine pubblico	Autorizzazioni di pubblica sicurezza
		Verbali degli accertamenti nei diversi settori (edilizio, sanitario, commerciale, etc.)

TITOLO X – TUTELA DELLA SALUTE

Classe		**Tipologie documentarie**
1	Salute e igiene pubblica	Autorizzazioni sanitarie
		Concessioni di agibilità

TITOLO XI – SERVIZI DEMOGRAFICI

Classe		**Tipologie documentarie**
1	Stato civile	Registro dei nati
		Registro dei morti
		Registro dei matrimoni
		Registro di cittadinanza
2	Anagrafe e certificazioni	Registro della popolazione
		Registro dell'Anagrafe degli italiani residenti all'estero
4	Polizia mortuaria e cimiteri	Registri di seppellimento
		Registri di tumulazione
		Registri di esumazione
		Registri di estumulazione
		Registri di cremazione
		Registri della distribuzione topografica delle tombe con annesse schede onomastiche

TITOLO XII – ELEZIONI E INIZIATIVE POPOLARI

Classe		**Tipologie documentarie**
2	Liste elettorali	Verbali della commissione elettorale
		Verbali del responsabile dell'ufficio elettorale
		Verbali della sottocommissione elettorale circondariale